Consumer Informational Privacy

Beke, Frank T.; Eggers, Felix; Verhoef, Peter C.

Published in:
Foundations and Trends® in Marketing

DOI:
10.1561/1700000057

Foundations and Trends® in Marketing

Consumer Informational Privacy: Current Knowledge and Research Directions

Suggested Citation: Frank T. Beke, Felix Eggers and Peter C. Verhoef (2018), "Consumer Informational Privacy: Current Knowledge and Research Directions", Foundations and Trends® in Marketing: Vol. 11, No. 1, pp 1–71. DOI: 10.1561/1700000057.

Frank T. Beke
University of Groningen, The Netherlands
f.t.beke@rug.nl

Felix Eggers
University of Groningen, The Netherlands
f.eggers@rug.nl

Peter C. Verhoef
University of Groningen, The Netherlands
p.c.verhoef@rug.nl

now
the essence of knowledge
Boston — Delft

Contents

Consumer Informational Privacy: Current Knowledge and Research Directions

Frank T. Beke[1], Felix Eggers[2] and Peter C. Verhoef[3]

[1] *University of Groningen, The Netherlands; f.t.beke@rug.nl*
[2] *University of Groningen, The Netherlands; f.eggers@rug.nl*
[3] *University of Groningen, The Netherlands; p.c.verhoef@rug.nl*

ABSTRACT

In the current *age of information* and *big data*, consumer informational privacy has become an important issue in marketing. Besides being worried about the growing collection, storage, and use of personal information, consumers are anxious about a lack of transparency or control over *their* personal data. Despite these growing concerns, understanding of how firms' privacy practices affect consumers remains limited. We review the relevant literature on consumer privacy from a marketing perspective and summarize current knowledge about how information collection, information storage, information use, transparency, and control influence consumers' behavior. In addition, we discuss to what extent the influence of firms' privacy practices differs between firms, consumers, and environments. On the basis of this knowledge, we formulate several hypotheses aimed at providing direction for future research regarding the role of consumer informational privacy in marketing.

Frank T. Beke, Felix Eggers and Peter C. Verhoef (2018), "Consumer Informational Privacy: Current Knowledge and Research Directions", Foundations and Trends® in Marketing: Vol. 11, No. 1, pp 1–71. DOI: 10.1561/1700000057.

1

Introduction

We are living in the *age of information*. Since firms started to realize that data could generate value for them and for their customers, they began collecting, storing, and using more data (or information) about consumers. Every year 16.1 trillion gigabytes of data are recorded, and forecasts are that this will grow to 163 trillion gigabytes by 2025 (Reinsel *et al.*, 2017). Consumer data allow firms to better understand their customers and provide products and services that better match consumers' need and preferences. Customer relationship management, customer intelligence, and, more recently, one-to-one marketing have all emerged by virtue of collecting information (Rust and Huang, 2014).

However, controversial revelations regarding the expansion of information collection and privacy in general (e.g., Edward Snowden's disclosures about data collection and surveillance programs) has resulted in a worldwide surge of privacy concern. In the United States, 92% of consumers worry about their online privacy (TRUSTe, 2016), while globally 57% of consumers were more concerned about their privacy compared to last year (CIGI-Ipsos, 2017). These concerns could deter consumers from accepting information collection, which matters even more in times in which privacy legislation and technological innovations —

such as cookie blockers and privacy-protective browsers — provide consumers more control over their privacy. For example, a recent study by Pew Research shows that 60% of consumers have chosen to not install an app when the collection of information was considered excessive, while 43% have uninstalled an app after finding out about excessive information collection (Olmstead and Atkinson, 2015). Even when consumers might not immediately abandon firms that neglect privacy it could result in bad publicity and a loss of trust in case consumers find out about the collection, storage, and use of information afterwards. For example, when consumers became aware Samsung was recording all interactions with their "smart" TVs, criticism went as far as accusing Samsung of spying on their customers (Forbes, 2015). Given the importance of information for firms, understanding how privacy affects consumers, and, more specifically, when and why consumers accept or reject the collection, storage, and use of information, has become crucial for the field of marketing (Wedel and Kannan, 2016; Montgomery and Smith, 2009).

Despite the growing attention for privacy, the understanding of how firms' privacy practices affect consumers and their relationships with firms is in its infancy. As privacy is an interdisciplinary topic, the knowledge about privacy and information disclosure is dispersed across scientific domains, ranging from social psychology to information systems and public policy. Within marketing, privacy has mainly been studied in the direct or interactive marketing literature (Culnan, 1995; Nowak and Phelps, 1995; Milne and Boza, 1999; Schoenbachler and Gordon, 2002; Phelps *et al.*, 2000; Milne and Gordon, 1993), as part of service quality (Parasuraman *et al.*, 2005; Wolfinbarger and Gilly, 2003), or, more recently, in the literature on online advertising (Tucker, 2014; Bleier and Eisenbeiss, 2015a; Schumann *et al.*, 2014; Goldfarb and Tucker, 2011a). Although Peltier *et al.* (2009) and Martin and Murphy (2017) have provided a global overview on the role of privacy within marketing, due to their broad focus the specific understanding of how firms' privacy practices affect consumers need to be elaborated. While Lanier and Saini (2008) address part of this void by discussing (some) firm-related privacy issues, we believe a more structured overview focused on the influence of firms' privacy practices on consumers is

necessary. Specifically, firms need a more detailed understanding of when and why consumers are (un)willing to disclose information and how a firm's privacy strategy affects the relationship with their customers, such as when customers might consider switching to a competing firm. We therefore focus on how firms' privacy practices have an impact on consumers, their privacy concerns, and the exchange of information.

Our objective of this paper is twofold. First, we use current knowledge about privacy and information disclosure to outline the main empirical findings regarding the influence of firms' privacy practices on consumers' behavior.[1] In doing so, we also discuss how the influence of firms' privacy practices on consumers differs between firms, consumers, and contexts. Second, drawing on current knowledge we identify areas in need of further research and formulate hypotheses for them. We start by conceptualizing consumer informational privacy and then derive a conceptual framework, which guides the subsequent sections.

1.1 Conceptualization of consumer informational privacy

In light of the rise of photography and growing circulation of newspapers at the beginning of the 20th century, legal scholars Warren and Brandeis (1890) stressed the importance of privacy as "*the right to be let alone*." Besides preventing others from intruding an individual's personal sphere, such as their house, they also stated that every individual should be protected against improper publications. While the initial focus was on others being physically present in someone's personal sphere (physical privacy), the growing collection, storage, and use of personal information[2] has shifted the attention to informational privacy (Goodwin, 1991; Rust *et al.*, 2002; Mason, 1986). Informational privacy intrusion relates to others monitoring and recording an individual's behavior, and thus to the collection and storage of information, without necessarily being physically present. Meanwhile, protection from improper publications

[1] Given our focus on empirical findings we exclude papers describing economic models (for an overview, see Acquisti *et al.*, 2016) or exploring the influence of public policy on firms (Miller and Tucker, 2009; Adjerid *et al.*, 2016).

[2] In line with recent legislation, we consider personal information to be all information that can be attributed to one individual (General Data Protection Regulation (EU), 2016).

relates to how the information is being used. The growing importance of consumer information directs the focus throughout this paper to informational privacy of consumers, to which we will simply refer to as *privacy*.

There has been much discussion on how privacy should be defined. Some scholars have suggested that privacy is context-specific so that it cannot be generally defined (Martin and Murphy, 2017; Pavlou, 2011; Smith *et al.*, 2011). This literature stream has proposed to focus on harmful activities using information instead (Prosser, 1960; Solove, 2006), whereby context-specific norms determine whether activities are harmful and thus violate privacy (Nissenbaum, 2004). Despite these suggestions, we follow the juridical standpoint that privacy is matter of autonomy and control over the collection, storage, and use of information (Westin, 1967; Altman, 1975; Petronio, 1991; Stone *et al.*, 1983; Smith *et al.*, 1996; Malhotra *et al.*, 2004). Recent privacy laws and guidelines in the United States and the European Union have also adopted this standpoint on privacy, as they aim to let consumers decide for themselves what happens with *their* information. This implies that privacy is only violated when information is collected, stored, or used against the consumer's will. Consumers' *effective* control depends on being aware of and having the ability to influence the collection, storage, and use of information (Goodwin, 1991; Foxman and Kilcoyne, 1993; Caudill and Murphy, 2000). Therefore, in the context of firms and consumers we define privacy as *the extent to which a consumer is aware of and has the ability to control the collection, storage, and use of personal information by a firm*. Thus, if firms want to respect consumers' privacy they should explain what information they collect, how they store the information, and for which purposes they will use the information (transparency). Moreover, firms should allow consumers to prevent firms from collecting information, to have them discard information, and to prohibit them from using their information (control).

Across a wide range of disciplines, ranging from social psychology to information systems and, more recently, marketing, there has been a debate about what privacy is and what privacy is not (Smith *et al.*, 2011; Spärck Jones, 2003). Because privacy is contingent on control, knowingly disclosing information or accepting information collection

is not a violation or deterioration of privacy. This implies that, unlike prior suggestions (Rust *et al.*, 2002; Posner, 1981; Posner, 1978), we consider privacy not the same as concealing or withholding information. Although related, privacy is also not the equivalent of security, as that implies that (unknown) outsiders illegally — that is, without proper authorization — intercept or access information (Belanger *et al.*, 2002; Martin *et al.*, 2017; Hoffman *et al.*, 1999). Given that information is collected, stored, or used without consumers knowingly consenting when security fails, security can be considered as one requirement for ensuring privacy and will be treated as such.

1.2 Conceptual framework

Figure 1.1 presents our conceptual framework, which guides our discussion of the literature. We will discuss how firms' privacy practices, which encompasses the way firms handle the information and privacy of consumers, affects consumers' attitudes, intentions, and behavior. Specifically, we discern five privacy practices that matter to consumers: information collection, information storage, information use, transparency, and (consumer) control. Understanding when consumers withhold (or falsify) information, reject information collection, or even refuse to interact or transact with a particular firm owing to its privacy practices has become crucial for managers. Moreover, firms need to know how consumers are affected when confronted with the storage and use of personal information, through marketing communication or location-based services.

Consumers' attitudes or perceptions with regard to privacy, such as privacy concern, often mediate the effect of firms' privacy practices on consumers' intentions or behavior. Therefore, many studies have used these attitudes or perceptions either as proxies for firms' privacy practices (predictor) or as surrogates for consumer behavior (outcome). What complicates matters is that the influence of firms' privacy practices on consumers could differ between firms, consumers, and environments. For example, consumers accept the collection of medical information more easily when done by healthcare providers (firms), when being in

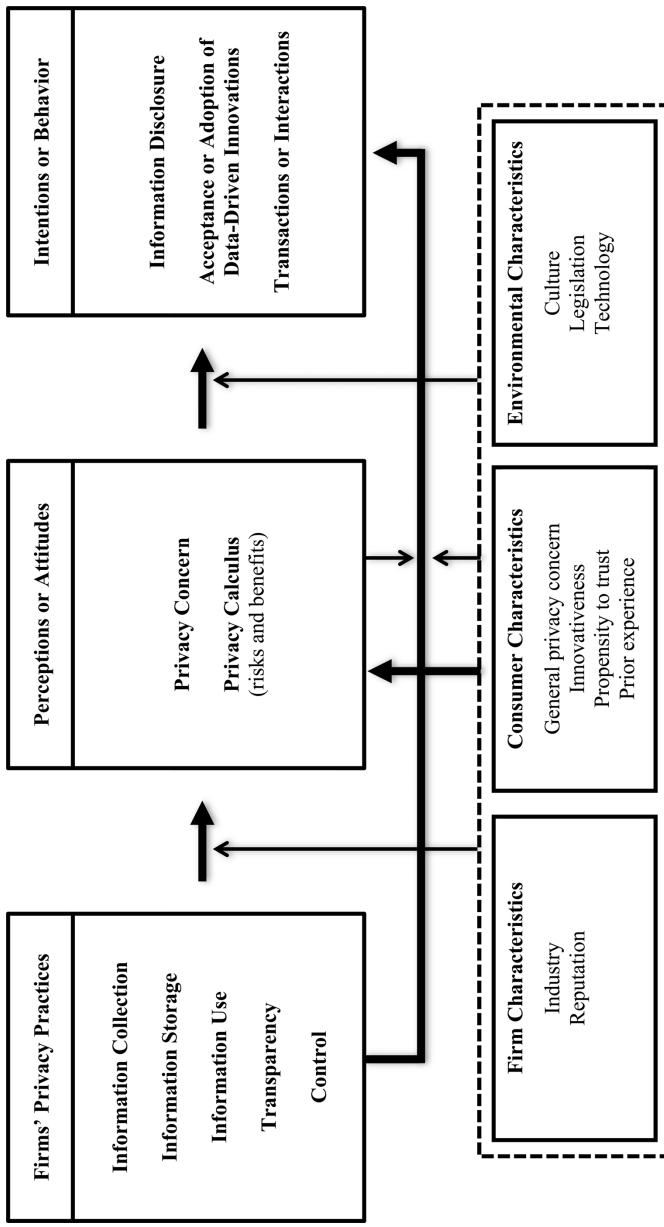

Figure 1.1: Conceptual framework.

perfect medical condition (consumers), or when privacy is regulated (environment).

To explain the influence of firms' privacy practices on consumer behavior, most studies have focused on the construct of privacy concern. Although conceptualized and operationalized in various ways, privacy concern always captures consumers' perceptions (or attitudes) of how the collection, storage, and use of personal information, or (lack of) transparency or control, negatively affect them (Smith *et al.*, 1996; Malhotra *et al.*, 2004). Whereas the collection, storage, and use of personal information matter due to the negative consequences consumers may endure (distributive fairness), social contract theory suggests that transparency and control also matter as consumers also take the procedures and interpersonal treatment (procedural fairness) into account (Donaldson and Dunfee, 1994). The importance of transparency and control is also established in reactance theory, which proposes that consumers resist being restricted in their choices (Brehm, 1966). In the context of privacy this implies that consumers will respond positively (negatively) when they believe firms are (not) transparent and provide (no) control over the collection, storage, and use of personal information (Culnan and Bies, 2003; Son and Kim, 2008). Besides privacy concern, Table 1.1 provides an overview of related constructs scholars have used to capture consumers' worries or uneasiness (attitudes and perceptions), such as privacy risk (Featherman *et al.*, 2010), perceived privacy (Dinev *et al.*, 2013), information sensitivity (Mothersbaugh *et al.*, 2012), intrusiveness (Li *et al.*, 2002; Burgoon *et al.*, 1989), and vulnerability (Martin *et al.*, 2017).

Prior work has applied various theoretical frameworks to explain why consumers disclose information despite being concerned. Consumers' ability to protect their own privacy (protection motivation theory) (Rogers, 1975; Youn, 2009), or their trust in specific firms (Morgan and Hunt, 1994; Wirtz and Lwin, 2009) might diminish consumers' concerns in a specific context. More recently the rationale that consumers look beyond the negative outcomes (concerns), and also take the positive outcomes of the collection, storage, and use of personal information into account, has taken root. Being closely related to social exchange theory (Homans, 1958; Premazzi *et al.*, 2010) and expectancy theory

Table 1.1: Privacy concern and related constructs.

Construct	Definition	Source
Privacy concern	A consumer's worries or uneasiness with regard to the collection, storage, and use of personal information, or (a lack of) transparency and control	Smith *et al.* (1996) and Malhotra *et al.* (2004)
Privacy risk	Subjective assessment of potential losses of confidential personally identifying information, including potential misuse	Featherman *et al.* (2010)
Perceived privacy	An individual's self-assessed state in which external agents have limited access to information about him or her	Dinev *et al.* (2013)
Information sensitivity	The potential loss or risk for consumers when information is disclosed	Mothersbaugh *et al.* (2012)
Intrusiveness	The extent to which an individual perceives unsolicited invasion in his or her personal sphere	Burgoon *et al.* (1989)
Vulnerability	Perception of susceptibility to harm owing to unwanted use of personal data	Martin *et al.* (2017)

(Vroom, 1964; Hann *et al.*, 2007), the privacy calculus suggests that consumers determine for themselves whether they regard the consequences of the collection, storage, and use of personal information to be beneficial (providing benefits) or detrimental (incurring costs or risks) in a specific situation (Laufer and Wolfe, 1977; Culnan and Armstrong, 1999; Dinev and Hart, 2006). These consequences can be tangible (e.g., monetary discount) or intangible (e.g., uncomfortable feeling), and have been explained using more generic theoretical frameworks, such

as the theory of reasoned action (Fishbein and Ajzen, 1975) or the technology acceptance model (Davis, 1989). The privacy calculus is however considered as the "*most useful framework*" to understand the acceptance of information collection (Culnan and Bies, 2003, p. 326). Since the privacy calculus can accommodate most theoretical frameworks it has seen many explicit or implicit applications (Mothersbaugh *et al.*, 2012; Premazzi *et al.*, 2010; Dinev and Hart, 2006; Xie *et al.*, 2006), and will serve as foundation for this review as well.

1.3 The privacy calculus and the privacy paradox

Despite the growing prominence of the privacy calculus, in some situations consumers' privacy attitudes or perceptions are inconsistent with their actual privacy-related behavior — a discrepancy that has been termed the *privacy paradox* (Berendt *et al.*, 2005; Norberg *et al.*, 2007). Researchers have offered various explanations for its existence (Acquisti *et al.*, 2015; Dinev *et al.*, 2015). Besides that some part of consumer behavior is inherently inconsistent or suffers from bounded rationality (Ariely, 2009), consumers' privacy concerns are seldom triggered. Especially in low-involvement situations, such as when consumers search online or use their mobile phone, the influence of biases and heuristics can be strong (Petty and Cacioppo, 1986; Chaiken, 1980). In other instances, consumers are unable to respond because they are unaware that information is being collected or used (Acquisti and Grossklags, 2005b), lack the ability to control firms' privacy practices (Turow *et al.*, 2009), or have no suitable alternatives.

Apart from irrational behavior or situations in which consumers are unaware or unable to exert control, the privacy paradox has also been a measurement issue. Given that consumers' privacy preferences are strongly influenced by situational or contextual characteristics (Nissenbaum, 2004), when and for which context privacy concern is measured matters — that is, privacy concern with regard to a specific technology (e.g., the Internet), a specific firm (e.g., Google), or a specific situation (e.g., when searching for a product). Moreover, benefits have either been ignored, measured incompletely, or using only very generic measures (e.g., Xu *et al.*, 2009; Xu *et al.*, 2011). In addition, the

consequences (benefits and costs) of the collection, storage, and use of information are not always immediate and definite (Brandimarte *et al.*, 2013), which suggests that the perceived probability of consequences should be taken into account (Risk Theory, Bauer, 1960; Conchar *et al.*, 2004). So we suggest that consumers' acceptance of the collection, storage, and use of personal information is best explained by their context-specific perception of the benefits and costs, taking into account transparency, control, and the uncertainty of these benefits and costs.

Hypothesis 1: Consumers' acceptance of the collection, storage, and use of personal information is best explained by their context-specific perception of the benefits and costs, taking into account transparency, control, and the uncertainty of these benefits and costs.

2

Information Collection

2.1 Type and amount of information

Nowadays, firms collect more information about their consumers than ever before. In general, the more information firms demand, the less willing consumers are inclined to provide them (Hui *et al.*, 2007). Consumers feel more vulnerable when firms have access to more information (more risk), which leads them to provide erroneous information, initiate negative word of mouth, or even switch firms (Martin *et al.*, 2017).

Firms collect information about consumers' online behavior (e.g., click-stream data, social media), offline behavior (e.g., transaction records, location data), and information needed for interactions or transactions (e.g., contact information, financial state). Consumers are affected by "what" firms want to collect, as they rather disclose lifestyle or purchasing habits than financial or medical information (Mothersbaugh *et al.*, 2012; Premazzi *et al.*, 2010; Lwin *et al.*, 2007). Consumers disclose less information when they consider information to be sensitive (Brandimarte *et al.*, 2013; Acquisti *et al.*, 2012; John *et al.*, 2011), with sensitivity increasing when the potential for loss (or risk) becomes greater (Mothersbaugh *et al.*, 2012). More recent work has shown that different types of information (e.g., financial information,

medical information) can result in different types of losses (e.g., monetary loss, social loss) (Milne *et al.*, 2017). Therefore, consumers may consider information as sensitive for various reasons. For example, disclosing embarrassing information (e.g., sexual fantasies) might result in a loss of face, while disclosing identifiable information (e.g., name) might result in a loss of anonymity (White, 2004). Understanding which types of information result in which types of losses, and which loss is considered most troublesome, would help firms mitigate consumers' concerns.

2.2 Information collection method

Besides *what* firms collect, also *how* they collect information matters. Digitalization has radically changed the way firms collect information about consumers. Rather than collecting information in person firms nowadays primarily gather information via computers or other information systems. Consumers respond positively when information is collected by computers rather than humans, such as employees (Schwaig *et al.*, 2013), as without humans involved consumers have a sense of anonymity (Tourangeau and Yan, 2007). Another consequence of digitalization has been that consumers have to decide whether they accept that firms collect information about them automatically rather than actively disclosing information themselves, for example, via forms. This shift makes the collection of information less visible, which could amplify the privacy paradox. Moreover, it has started to give consumers the feeling information is being collected behind their backs (Acquisti and Grossklags, 2005b), which could result in a backlash when consumers eventually learn that firms have collected their information without notifying them — that is, without transparency (see Section 5).

A recent development with regard to *how* firms collect information has been that, besides active and passive information collection, firms have increasingly begun to rely on making inferences about consumers. For example, firms could estimate consumers' income level based on prior purchases or search history. Despite that most (data-driven) firms make these inferences, and that such information could generate value for firms and their customers, consumers have, in the past, indicated opposition to inferred information (Culnan, 1993). Whether this is

generalizable and what the underlying reason(s) are remains unclear. One issue could be that because inferences are not factual information, consumers fear they might be inaccurate. This fear might be mitigated in the future with more widespread implementations of increasingly accurate machine-learning techniques and consumers' experiences with the inferences made. Moreover, making inferences might indicate that firms are hesitant to ask consumers for this information directly, which suggests the information is either sensitive or potentially negative in its effects on consumers. Finally, consumers might oppose inferences because they lack any control over when and which inferences firms make.

Hypothesis 2: Consumers oppose firms generating information by making inferences because (1) inferences might be inaccurate, (2) inferences might affect consumers negatively, or (3) they consider making inferences to be unfair.

2.3 Online vs. Offline behavior

Besides that digitalization enables firms to closely monitor how consumers behave online, more recently mobile phones and other *smart* devices have provided firms with access to information regarding consumers' offline behavior. In the past, consumers have indicated to worry more about their offline identity (*real life*) than about their digital identity (*virtual life*) (Acquisti and Grossklags, 2005a). For example, when Google initially announced they would start monitoring consumers' offline behavior via their "smart" home device, consumers expressed their concerns (Huffington Post, 2017). Therefore, consumers are expected to be reluctant towards firms monitoring how they behave in stores (e.g., via RFID), on the road (e.g., via GPS), or in their own home (e.g., via a "smart" home device). If firms want to deal with this reluctance they need more insights as to when and why this is the case.

Contextual integrity and the influence of context-specific norms (Nissenbaum, 2004) provide a reasonable explanation for consumers' reluctance towards allowing firms to monitor their offline behavior. The norm (and law) in most countries is that consumers should be able

to behave without others continuously watching over their shoulder, especially in consumers' personal sphere, such as their home. Consumers might not feel comfortable when firms monitor and record socially sensitive behavior, such as going to the bathroom.

Hypothesis 3: Consumers are more reluctant to let firms collect information about their offline behavior compared to online behavior, predominantly because consumers expect they can behave freely (i.e., without firms monitoring them) in their personal sphere, such as at home.

However, as the "virtual life" and "real life" are becoming less distinct, consumers have become less reluctant to firms monitoring their offline behavior. In fact, 44% of the US adults are planning to purchase a "smart" home device in 2018 (CTA, 2017). Future research should address why consumers have become less reluctant — for example if consumers have become more convinced of the benefits of firms using information about offline behavior (see Section 4). Moreover, growing acceptance of collecting offline information could also be a consequence of a different firm, with a better reputation, offering the service (see Section 7) or a change in generations (see Section 8).

2.4 Monetary compensation and other persuasion methods

Without changing the *what* and the *how* of information collection, and in line with the privacy calculus, firms have convinced consumers to disclose information by compensating them with additional benefits or monetary incentives. Some of these benefits are linked to information use, such as the ability to personalize products or services (see Section 4). Also unrelated incentives, such as discount vouchers or access to free content, can persuade consumers to disclose information (Premazzi *et al.*, 2010; Hui *et al.*, 2007) or let firms track their behavior (Acquisti *et al.*, 2013; Derikx *et al.*, 2016). Preliminary evidence suggests that monetary compensation gives consumers the feeling that they are *selling* their information, so they expect less control and allow firms to use the information any way they like (Gabisch and Milne, 2014). The attractiveness of monetary benefits is also reflected in consumers'

adoption of loyalty programs. Multiple studies have shown that although consumers are worried about their privacy, discounts and other monetary benefits convince them to adopt loyalty programs nonetheless (Dorotic *et al.*, 2012; Demoulin and Zidda, 2009; Leenheer *et al.*, 2007).

However, providing monetary compensation becomes less effective when the risks of sharing information become higher — an effect that depends on both the amount and the type of information. Moreover, preliminary evidence suggests that insufficient monetary compensation could arouse consumers' privacy concern (Andrade *et al.*, 2002), and that monetary compensation could deter consumers from disclosing information when the information is incongruent with the products and services of the firm (Li *et al.*, 2010). Therefore, firms have to be cautious when offering a monetary compensation, as we expect that its effectiveness depends on the amount and type of information firms want to collect. Future research should clarify the boundary conditions for monetary compensation, and should assess to what extent the effectiveness of monetary compensation differs between firms and consumers.

Hypothesis 4: Monetary compensation becomes less effective (or even detrimental) for increasing consumers' willingness to disclose information when firms want to collect (1) more information, (2) more sensitive information, or (3) incongruent information.

Besides monetary compensation, there are other ways for firms to persuade consumers to disclose information. For example, consumers disclose more information in unprofessional environments in which privacy is triggered less (John *et al.*, 2011), and, driven by comparative judgment, they disclose more when they believe other consumers have disclosed similar information (Acquisti *et al.*, 2012). Similarly, when computers disclose information first consumers reciprocate by also disclosing information (Moon, 2000; Zimmer *et al.*, 2010). Besides these methods, we believe that firms could also persuade consumers to accept information collection by collecting information in small steps. Individuals do not always take in gradually increasing risks (Slovic, 2000), which suggests that firms could benefit from collecting less or less sensitive information from consumers first before requesting more or

more sensitive information. Although, in surveys, respondents provide more answers when intrusive questions are asked first (Acquisti *et al.*, 2012), firms might be better off gradually increasing the amount or the sensitivity of information requested, as otherwise they might scare off consumers when they immediately want to collect sensitive information.

3

Information Storage

3.1 Security breach

After collecting information about consumers, firms have to decide how and where to store the information. One aspect that matters to consumers is that unknown outsiders cannot gain unauthorized access to their personal information (Smith *et al.*, 1996). Therefore, information storage relates closely to security. Over the past years, security breaches have become more common. In 2016, US firms and government agencies suffered over 1,000 security breaches, an increase of 40% compared to the year before (Bloomberg, 2016). In the short term, these security breaches have shown to negatively affect stock prices (Martin *et al.*, 2017; Acquisti *et al.*, 2006; Cavusoglu *et al.*, 2004; Malhotra and Kubowicz Malhotra, 2011), with the negative effect becoming stronger when the security breach becomes more severe, that is more victims or more data leaked (Martin *et al.*, 2017; Acquisti *et al.*, 2006). Moreover, owing to spillover effects, firms' stock prices might decrease when competing firms suffer a security breach, although a spillover effect reverses when the security breach becomes more severe (Martin *et al.*, 2017). However, it should be noted that in the long term these security breaches seem to have no effect on stock prices. While Malhotra and Kubowicz Malhotra

(2011) found that 30 days after the announcement of a security breach stock prices are still significantly lower, a more recent study shows that after one or two years the security breach has no significant effect on stock prices (Martin *et al.*, 2017).

In addition to affecting stock prices, security breaches also directly affect consumers by raising their general privacy concern (Smith *et al.*, 1996; Malhotra *et al.*, 2004; Malhotra and Kubowicz Malhotra, 2011; Bansal *et al.*, 2015, see Section 8). Preliminary evidence suggests that when confronted with a security breach consumers are also more inclined to falsify information, commence in negative word-of-mouth, and even switch firms (Martin *et al.*, 2017).

Examining consumers' behavioral reaction towards security breaches in more detail, future research should assess how firms can diminish the negative effect of security breaches. With regard to stock prices, the adverse effect of a security breach was shown to be less severe when a third party rather than the focal firm was held responsible or when the security breach was caused by an accident rather than a deliberate attack (Acquisti *et al.*, 2006). Moreover, firms that are transparent about their privacy practices and provide consumers with control over these practices in general, even before outsiders gain unauthorized access, suffer less from the impact of a security breach (Martin *et al.*, 2017). Whether these possibilities also affect the impact of a security breach on the way consumers behave remains to be seen.

3.2 Safer storage

In line with risk theory (Peter and Tarpey, 1975), we believe firms have two options for lowering the risk of security breaches. One is to decrease the impact of security breaches for consumers by reducing the potential loss for consumers, for example, by storing less or less sensitive information. The impact of a security breach can also be diminished by anonymizing or aggregating the information (Verhoef *et al.*, 2016). Anonymization requires that firms remove the link between a person and that person's information, by removing identifying information such as name or e-mail address (Acquisti *et al.*, 2016). Aggregation means that information about consumers is stored at the group or segment level,

which per definition implies that the information is anonymous. While anonymization or aggregation ensures that individual consumers are not harmed when information falls into the hands of unknown outsiders, the downside is that it limits firms' ability to create additional value using the information (Schneider *et al.*, 2017), although there are possibilities to take full advantage of consumer information while simultaneously protecting consumers' privacy (Holtrop *et al.*, 2017).

The alternative is to make security breaches less likely by decreasing the likelihood of a negative event. Firms might store the information for a shorter period, or assure consumers that their information is collected and stored in a *safe* environment (Hann *et al.*, 2007). For example, Dutch telecom operator KPN tried to convince consumers that its cloud services were less likely to result in privacy issues because its servers were located in the Netherlands and thus fell under the strict data protection regulation of the EU (BTG, 2012). While these measures might diminish the likelihood of a security breach, the pledge to store information in a *safe* environment only works when consumers are convinced an environment is safer (Sutanto *et al.*, 2013), and thus believe that a privacy breach or violation is indeed less likely in that environment. Future research should not only focus on examining how information storage affects consumers in general, but also make more specific what convinces consumers that information storage is *safe*.

Hypothesis 5: Consumers are more willing to let firms store information when firms promise to store (1) less or less sensitive information, (2) only anonymized or aggregated information, (3) information for a shorter period, or (4) information in a safe environment.

4

Information Use

4.1 Aggregated level and individual level

Once collected and stored, firms use the information about consumers for various purposes. As for the collection and storage of information, the use of information only affects consumers when firms clearly inform them as to how the information is used, or when the use of information is evident to consumers. On an aggregated level, firms use consumer information to monitor or optimize internal processes, or to enhance their understanding of the needs and preferences of consumers in general (Wedel and Kannan, 2016). Besides being less evident to consumers, such information use has limited impact on consumers' privacy because it does not rely on personal information, and therefore the influence on consumers is often negligible. Even when firms notify consumers about using information on an aggregated level consumers are inclined to accept as long as they consider it beneficial to themselves. As an example, consumers accept the use of RFID tags in retail outlets when firms use the information in order to reduce empty shelves (Smith *et al.*, 2014).

On an individual level, besides that firms need information about consumers to deliver products or notify consumers about changes in their

service, firms have begun using the information about consumers for personalization. Personalization implies that firms tailor their offerings of products and services to the needs and preferences of individual consumers (Montgomery and Smith, 2009; Adomavicius and Tuzhilin, 2005), thereby increasing the relevance of their products and services. The increasing digitalization enables firms to personalize their entire marketing mix, allowing to individualize products or services, prices, promotions, and places or locations (Rust and Huang, 2014). While consumers might oppose personalization when (they believe) it puts them at a disadvantage — that is, when they have to pay more or receive inferior services compared to other consumers (Lacey *et al.*, 2007) — our focus will be on how privacy (concern) might affect the approval of personalization (Rust and Huang, 2014; Montgomery and Smith, 2009).

4.2 Personalization of product or service

To differentiate themselves from their competitors, firms continuously search for ways to use information to augment their products and services. For example, firms might remember contact details or payment preferences to expedite the checkout (Acquisti and Varian, 2005). These enhanced services benefit both firms and consumers — consumers from more relevant products and services, firms from more loyal and committed customers (Coelho and Henseler, 2012). Consumers are more (less) inclined to show promotion-focused (prevention-focused) behavior when firms use the information to personalize the website interface (Wirtz and Lwin, 2009). Moreover, website morphing, which entails personalizing websites to individual consumers, has a positive effect on consumers' purchases (Hauser *et al.*, 2014). In addition, consumers respond positively to personally recommended music (Chung *et al.*, 2009) and news (Chung *et al.*, 2016). Besides personalized recommendations, such as Amazon's "*recommended for you*," LinkedIN's "*suggested connections*," or Netflix' "*selected for you*," more recently consumers have also benefited from other forms of personalized content or insights, such as Fitbit's *fitness insights* or Siemens's *smart energy meter*.

However, the growing personalization also has resulted in tension between the relevance and the collection and use of (more) information. Even when consumers are not always aware which information firms need for these personalized services, the amount and type of information needed affects consumers' acceptance of personalization. More specifically, consumers value personalized service less when it is based on sensitive information (Mothersbaugh *et al.*, 2012), and preliminary evidence shows that for recommendation systems consumers only disclose information when they expect valuable recommendations (Knijnenburg and Kobsa, 2013). Moreover, while external information — such as derived from social media — could improve personalization (Chung *et al.*, 2016), even in the context of scientific research many respondents were hesitant to provide access to such information to improve product recommendations (Heimbach *et al.*, 2015). The context of search-and-discovery services, such as FourSquare or Gowalla, provides further evidence that consumers' acceptance of personalized services depends on which information is needed (Xie *et al.*, 2014). In line with the privacy calculus, consumers seemingly balance the positive and negative consequences of personalized services. Future research should assess the optimal balance between relevance and privacy, and study when and for which consumers the benefits outweigh the *costs*.

4.3 Personalization of price

Besides personalized products or services, firms have begun providing consumers personalized discounts or rewards, and even personalized prices (Acquisti and Varian, 2005). Even though personalized promotions might benefit firms (Zhang and Wedel, 2009; Khan *et al.*, 2009), consumers have shown to value personalized discounts less when based on sensitive information — that is, discounts for *embarrassing* products (White, 2004). Rather than being worried about their privacy, consumers disapprove personalized pricing when they fail to understand why they pay more than other consumers and consider it unfair when they receive higher prices (Feinberg *et al.*, 2002). Personalized prices rely mostly on firms' inferences about consumers' willingness-to-pay instead of factual information. In addition to the negative consequences of higher prices

or fairness concerns, consumer might also worry about the accuracy of the inferences (see Section 2.2). Preliminary evidence about firms experimenting with personalized pricing (e.g., outrage over Amazon's variable pricing dropped their stock price by more than 13%, CNN, 2005) shows that firms can suffer from (future) backlash when consumers find out that prices are consumer-specific.

4.4 Personalization of promotion

Although the personalization of online (banner) advertisements and direct mailings to individual consumers has become standard practice, consumers have shown mixed feelings towards the personalization of marketing communication. While consumers consider personalized marketing content more relevant and useful, thereby making banner ads and direct mails more effective (Tucker, 2014; Bleier and Eisenbeiss, 2015a; Goldfarb and Tucker, 2011a; Aguirre *et al.*, 2015; Van Doorn and Hoekstra, 2013; Ansari and Mela, 2003; Bleier and Eisenbeiss, 2015b), a majority of US consumers still rejects behavioral targeting (Purcell *et al.*, 2012).

Therefore, when confronted with banner ads and direct mails, too much personalization makes marketing communication intrusive and triggers privacy concerns (Li *et al.*, 2002; Van Doorn and Hoekstra, 2013; Edwards *et al.*, 2002). As consumers become cognizant information is collected and used, reactance theory suggests consumers are bothered by a lack of control over the collection or use of information for personalized marketing communication. Besides that ads become more intrusive when they are cognitively intense or incongruent with the website (Li *et al.*, 2002; Edwards *et al.*, 2002), intrusiveness is induced when firms openly use detailed information about individual consumers in their ads (Aguirre *et al.*, 2015; Van Doorn and Hoekstra, 2013). Targeting ads to an individual consumer (Tucker, 2014) or showing the exact same product the consumer saw before, so-called dynamic retargeting, also makes online ads less effective (Bleier and Eisenbeiss, 2015b; Lambrecht and Tucker, 2013), as consumers become aware that personal information is being collected, stored, and used (Bleier and Eisenbeiss, 2015b).

As we will discuss in Section 5 (transparency) and Section 6 (control), firms can conserve the effectiveness of personalized marketing communication by becoming more transparent with regard to its creation (Aguirre *et al.*, 2015) or by providing consumers more control over information disclosure (Tucker, 2014). Moreover, firms could alter their marketing communication to try and reduce the arousal of privacy concerns. While not showing the exact same product twice (Bleier and Eisenbeiss, 2015b; Lambrecht and Tucker, 2013) and increasing the target audience of banner ads could prevent arousing privacy concern (Tucker, 2014), it would also diminish the match with individual consumers (and thus the effectiveness). In line with regulatory focus theory (Higgins, 1997), a better solution would be to try and avoid consumers getting into a prevention-focused state, and instead inducing a more promotion-focused state, by increasing the relevance of marketing communication. For example, personalizing online banner ads becomes more effective when a banner ad is more relevant to the consumer (Lambrecht and Tucker, 2013), and mobile ads become less intrusive (and more effective) when these ads are relevant with regard to the physical location of the consumer (Luo *et al.*, 2014). This way, firms might be able to alter the balance in favor of personalized marketing communication.

Hypothesis 6: Firms can preserve effectiveness of personalized marketing communication by getting consumers in a more promotion-focused state, for example, by making marketing communication, such as banner ads and direct mail, more relevant.

4.5 Personalization of place or location

A recent development is that the rise of mobile devices enables firms to personalize the location where they offer their products or services. Location-based services tailor content to consumers' physical location, thereby providing consumers with the convenience of receiving content at the right time and location (Xu *et al.*, 2009; Xu *et al.*, 2011; Zhao *et al.*, 2012). This content can range from location-specific information, such as weather reports, to location-specific advertisements or mobile

coupons. Given that location tracking has only recently gained attention, few studies have assessed the acceptance of location-based products and services.

However, as also discussed in Section 2, while consumers are vigilant about firms tracking offline behavior, a majority of consumers still rejects location-based advertising (Urban and Hoofnagle, 2014). Therefore, firms need a better understanding of the tension between relevance and privacy in the context of location-based products and services. More specifically, firms need to understand when consumers value the savings in time or effort enough to offset their worries about firms tracking their location. What seems to matter most to consumers is whether the content firms provide is truly relevant to them, as the intention to disclose information to location-based services is explained more by the benefits (incentives, possibility to interact) than the costs (privacy concern) (Zhao *et al.*, 2012). Even more than online personalization location-based services might give consumers the feeling they are being followed and watched. Firms can prevent triggering such feelings by making the information truly relevant, in terms of time and geographic location (Luo *et al.*, 2014), thereby bringing consumers in a more promotion-focused state. Thus, as long as firms provide relevant content, consumers are influenced less by negative feelings with regard to location tracking.

4.6 Third-party sharing

Besides using information internally, firms can also generate revenue by selling information or customer intelligence to other firms. Consumers oppose sharing and selling information to unknown third parties (Alreck and Settle, 2007), as they believe they are more at risk (Jai *et al.*, 2013), most likely because they do not know (transparency) or cannot influence (control) how their information will be used. Moreover, third-party firms typically have no incentive to provide consumers with any suitable benefit in return. As a result, consumers respond negatively to firms selling information, for example, by complaining, refusing information disclosure, or avoiding marketing communication, whereas

their long-term commitment and loyalty are enhanced when firms refuse to sell information to third parties (Wirtz and Lwin, 2009). Although firms could try and appease consumers' concerns, for example, by disseminating information with less detail, the issue is that this decreases the potential benefit of information sharing (Schneider *et al.*, 2017).

5

Transparency

5.1 Effect on consumers

Over the past decades, pressure from legislators and consumer protection commissions has coerced firms to become more transparent about their privacy practices. In line with social contract theory, transparency enhances the relationship between firms and consumers as it ensures a *fair exchange* of information (Culnan and Bies, 2003). Therefore, transparency decreases the extent to which consumers feel their privacy is violated (Martin *et al.*, 2017), and makes consumers more willing to disclose information (Son and Kim, 2008) or even purchase products (Schlosser *et al.*, 2006).

Social contract theory also suggests that firms could benefit long-term when consumers consider them transparent due to enhanced trust and commitment (Culnan and Bies, 2003). We suggest that transparency could prevent future discontent with firms' privacy practices, as consumers know or could have known how their privacy was handled. This shifts (part of) the responsibility for future privacy issues or the *locus of control* from the firm to the consumer. Likewise, when firms explain their privacy practices, consumers are less likely to regret giving

permission to collect, store, or use their information, as it increases the correspondence between consumers' intentions and their behavior (Zimmer *et al.*, 2010). Future research should examine this (long-term) effect more carefully, and assess whether and why consumers become more committed and loyal to firms they consider transparent.

Hypothesis 7: Transparency about how consumers' privacy is handled diminishes future discontent with firms' privacy practices.

5.2 Privacy statement and seal

To notify consumers about the collection, storage, and use of information most firms post a privacy statement, which is a written overview of their privacy practices generally available on their website. An issue for firms is that consumers do not always take the effort to understand how firms handle their privacy. Especially online or on mobile devices consumers have to make many decisions within a short period of time, and are faced with too much information about their privacy (*information overload*), which makes it difficult to understand which information is collected and stored, and how firms use this information (Metzger, 2007). Moreover, some consumers consider privacy not important enough to invest time in understanding a firm's privacy practices (Dinev *et al.*, 2015). Therefore, rather than reading privacy statements (Eurobarometer, 2011) consumers use them as a heuristic instead. In line with signaling theory (Boulding and Kirmani, 1993) prior studies have shown that the mere presence of a privacy statement increases consumers' trust in a firm (Aljukhadar *et al.*, 2010), willingness to disclose information (Xie *et al.*, 2006; Hui *et al.*, 2007; Wang *et al.*, 2004), and even willingness to purchase (Aljukhadar *et al.*, 2010). However, given that in most countries firms are required to post a privacy statement, the actual differentiating effect on how consumers behave is probably limited.

Likewise, firms post privacy seals, such as TRUSTe or BBBOnline, to try and convince consumers that their privacy is secure. Although some studies show that privacy seals give consumers the feeling that firms are transparent (Rifon *et al.*, 2005; Kim and Kim, 2011) and

increase trust more than other objective trustmarks (Aiken and Boush, 2006), other studies show that the effect on consumers' willingness to disclose information is small (Wang *et al.*, 2004) or absent, despite consumers' familiarity with the seal (Hui *et al.*, 2007). Still, a more recent study confirms that when choosing between firms consumers opt for the firm with a privacy signal (e.g., a privacy icon, link to privacy statement), even when that firm is more expensive (Tsai *et al.*, 2011).

5.3 Arousal of privacy concern

Another (related) reason why firms struggle with transparency is that privacy is not always top-of-mind, especially online or when consumers use mobile devices. Mentioning privacy, information collection, or other "sensitive" terms, such as behavioral targeting or RFID, triggers consumers' privacy concerns. For example, respondents disclose less information in surveys when privacy is mentioned (Acquisti *et al.*, 2012), and consumers are less willing to adopt a tracking system in a grocery store when RFID is in the name (Smith *et al.*, 2014). In fact, consumers consider the negative outcomes ("*information will be used against me*") as more likely when firms explain both benefits and risks of information disclosure (LaRose and Rifon, 2007), worry more about their privacy when "*data mining*" is explained (Bolderdijk *et al.*, 2013), and pointing out a privacy policy on an online social network decreased consumers' willingness to disclose their location (Knijnenburg *et al.*, 2013).

Nevertheless, as firms are required to explain their privacy practices, a better understanding how to handle the adverse effect of transparency is essential. A solution could be that when firms trigger consumers' privacy concern they need to convince consumers that they rigorously protect privacy or that consumers have control over their information (see Section 6). One possibility would be to make privacy statements look *strong*, for example, by promising confidentiality and guaranteeing protection against information theft (Schlosser *et al.*, 2006). Similarly, posting a privacy seal in addition to explaining the benefits and risks of information collection reduces the perceived risks (LaRose and Rifon, 2007), as that also provides consumers some assurance.

Hypothesis 8: Firms can resolve (part of) the issue of privacy arousal by using signals in their communication about privacy that give consumers the feeling they are protected.

5.4 Explaining the benefits

As also discussed in Section 4, regulatory focus theory suggests that another solution for the issue of privacy arousal could be to stress the benefits of information collection and use in order to direct consumers' attention towards these benefits (Higgins, 1997). For example, when the benefits of RFID are stressed consumers consider it more useful, while stressing the negative side makes consumers more worried about their privacy (Smith *et al.*, 2014). Recently, several news outlets (e.g., *Bild, The Guardian, Forbes*) have begun using pop-up announcements to explain how the collection of information enables them to both supply news for free and provide consumers with news that fits their needs. Consumers feel less vulnerable when firms justify the use of personal information (Aguirre *et al.*, 2015), and this feeling of security increases the click-through intention for personalized banner ads (Aguirre *et al.*, 2015) as well as for personalized mail (White *et al.*, 2008). Likewise, explaining the benefits of behavioral targeting to consumers increases the acceptance and actual click-through of targeted banner ads (Schumann *et al.*, 2014).

However, if firms want transparency to be helpful they have to understand when consumers take the effort to understand their explanations of the benefits, and how to motivate consumers in case they take little or no effort to understand these explanations. One easy solution is to make privacy statements with the costs and benefits short and easy to read (Pan and Zinkhan, 2006), rather than using very technical or juridical language. Another possibility to make things easier for consumers would be to explain privacy practices and the way consumers benefit in short, easy-to-follow videos, as implemented by news outlet *The Guardian*. Preliminary evidence suggests that posting a video could enhance consumers' trust in the firm and (indirectly) their intention to transact with that firm (Aljukhadar *et al.*, 2010). Furthermore, firms could benefit from first explaining the negative consequences

to consumers (e.g., *information collection decreases your anonymity*) before explaining the positive consequences (e.g., *you get a discount*), as that enhances consumers' willingness to disclose information (White *et al.*, 2014).

Besides motivating consumers to invest time in understanding firms' privacy practices firms also need to decide what they communicate. Besides the aforementioned influence of the collection and storage of information, firms need to understand which benefit(s) derived from the use of information (see Section 4) consumers appreciate the most. For example, when justifying the collection of personal information for behavioral targeting, rather than stressing the increased relevance of banner ads, firms are better off emphasizing that collection allows free products or services (Schumann *et al.*, 2014). Besides stressing the right benefits, Martin *et al.* (2017) suggest that transparency only benefits firms when they also provide consumers control.

Hypothesis 9: Firms can resolve (part of) the issue of privacy arousal by stressing the (right) benefits to consumers.

6

Control

6.1 Effect on consumers

As for transparency, pressure from legislators and consumer protection commissions has demanded that firms provide consumers control over their information. Being focused on informed consent and providing consumers the *right to erasure*, the European Union in particular intends to give consumers more control over *their* own information (General Data Protection Regulation (EU), 2016). Social contract theory suggests that firms benefit from providing control, considering it is another important requirement for a *fair exchange* of information between firms and consumers (Culnan and Bies, 2003). When consumers believe a firm provides control over (secondary) use they trust the firm more (Mosteller and Poddar, 2017) and feel less vulnerable (Martin *et al.*, 2017). Therefore, consumers are more inclined to choose that firm (Phelps *et al.*, 2000; Hann *et al.*, 2007), are more cooperative and committed towards that firm (Son and Kim, 2008; Mosteller and Poddar, 2017), and are more willing to disclose (sensitive) information for a personalized service (Mothersbaugh *et al.*, 2012). Moreover, control over the storage of information enhances the acceptance of behavioral advertising (Schumann *et al.*, 2014). On Facebook, the effectiveness

of banner ads even increased after they made it easier for its users to control their privacy (Tucker, 2014).

Although it has been shown convincingly that consumers are positively influenced by (perceived) control, future research should assess why consumers become more cooperative and committed. Prior studies have suggested that control provides consumers with a sense of autonomy, which matters since consumers react negatively when they are confined in their choices (Brehm, 1966). Related to this is that control might make consumers feel less vulnerable (Martin *et al.*, 2017) as it allows consumers to revoke these choices whenever they please, making their choices less consequential.

Hypothesis 10: Control over information makes consumers more cooperative and committed, because (1) control provides them with a sense of autonomy, and (2) it makes decisions less consequential.

6.2 Disruption of information collection

Despite the mounting legislative pressure, firms seems to remain reluctant to provide control. Besides that providing control over information could be technologically challenging, a negative consequence could be that consumers might disrupt the collection, storage, or use of personal information, which would prevent firms from taking full advantage of customer intelligence and *big data*.

Preliminary evidence shows that consumers already become more cooperative by a feeling of control over the use of information (Brandimarte *et al.*, 2013). This seems to suggest that consumers are not so much interested in disruption, but rather in having the ability to disrupt in case this is needed. To the best of our knowledge, however, there have been no recent studies on the extent to which consumers make use of their ability to control the collection, storage, and use of information. For example, while Facebook and Google (Android) have introduced more options to control privacy (Norberg and Horne, 2014), they have not published any statistics on how many consumers take advantage of this control. Therefore, future research is much needed in this context. For now, we can only conclude that consumers are expected to disrupt

the collection, storage, and use of personal information when becoming aware of the harmfulness of a firm's privacy practices, such as selling sensitive information to third parties, exceeds the benefits they offer.

6.3 Control over stored information

Besides increasing commitment and loyalty to a firm, providing control could create another mutual benefit. Consumers are worried that firms' databases contain errors (Smith *et al.*, 1996), either because enriching consumer profiles using inferences results in inaccuracies or due to consumers providing erroneous information themselves. Firms can avoid such issues by making information provision voluntary (Norberg and Horne, 2014), and can also solve such issues by giving consumers access to their personal information and allowing them to correct any potential errors (Hann *et al.*, 2007). As an example, Google increasingly allows users to alter (improve) the profiles used for personalized advertisements with regard to consumers' interests and preferences.

6.4 Information disclosure as default

Another important issue for firms remains *how* they should provide consumers with control. Offering an opt-out choice results in more consumers consenting to provide information than an opt-in choice (Johnson *et al.*, 2002), while it has no effect on consumers' purchase likelihood (Eastlick *et al.*, 2006). However, legislators tend to force a choice of opting in rather than opting out. Besides legislative pressure, firms also have to be aware that an opt-out choice, which essentially makes information disclosure the default, results in more cases in which they collect, store, and use information without consumers actively consenting. While firms might benefit from this in the short term — consumers initially consent — it could result in situations in which information is collected against the will of the consumer, which might affect consumers' satisfaction and long-term commitment negatively.

As with transparency, control could prevent future discontent with firms' privacy practices as it shifts (part of) the responsibility for future privacy issues to the consumer. If firms provide control over

information, and consumers make no use of this control, consumers can only blame themselves when firms' privacy practices are not in line with their preferences. In line with this reasoning, preliminary evidence suggests that control in conjunction with transparency is most effective in decreasing feelings of emotional violation and increasing trust, as well as in decreasing the negative effect of a privacy breach (Martin *et al.*, 2017). Future research should examine in more detail how firms could best provide control in a way that does not antagonize consumers.

Hypothesis 11: Firms that have information collection as the default (e.g., use an opt-out choice for information collection) will suffer from (more) dissatisfied customers in the long term.

7

Firm Characteristics

7.1 Industries

Consumers' privacy preferences and expectations differ between contexts (Nissenbaum, 2004; Martin and Nissenbaum, 2016b). Therefore, the influence of privacy practices on consumers differs between industries (or sectors). Privacy is a more pressing issue in industries that rely on collecting a large amount of information or sensitive information, such as healthcare providers or banking. Hence, all features that decrease privacy concerns or increase trust are more important in fostering consumers' willingness to disclose information to, and more generally, their willingness to interact or transact with firms from those industries (Pan and Zinkhan, 2006; Bart *et al.*, 2005).

Besides the sensitivity of information, consumers take into account whether the information that is collected, stored, and used is congruent with the products or services of a firm. Consumers are more willing to disclose particulars when they anticipate they will be asked to disclose that information (White *et al.*, 2014). Thus, collecting sensitive specifics is less of an issue when the information is congruent with the firm's products or services. For example, while consumers accept that financial institutions will collect details about their income or mortgage they are

reluctant to disclose their medical condition (Lwin *et al.*, 2007; Martin and Nissenbaum, 2016b).

Moreover, the industry (or sector) also moderates the influence of security breaches, although these findings have not always been consistent. While Acquisti and colleagues (2006) show that the effect on firms is more severe for retail firms than for other firms (e.g., financial), a more recent study provides evidence that the effect is stronger for financial firms than for other firms (e.g., retail) (Malhotra and Kubowicz Malhotra, 2011). Moreover, Cavusoglu and colleagues (2004) showed earlier that the effect is more severe for online firms than for offline firms, most likely because for online firms there is more information to be lost. While these findings are all focused on stock prices future research should assess whether the direct influence of security breaches on consumers also differs between industries.

7.2 Reputation

Besides the industry, several other firm characteristics influence consumers. All characteristics of firms or websites that signal competence and quality, in particular their reputation, motivate consumers to disclose information (Schoenbachler and Gordon, 2002; Xie *et al.*, 2006; Aiken and Boush, 2006; Bart *et al.*, 2005; Lwin *et al.*, 2016).

Reputation also moderates the influence of firms' privacy practices. On the one hand, privacy statements are more effective for firms with a strong reputation (Xie *et al.*, 2006), as consumers have more confidence in the credibility of these statements. On the other hand, transparency is more crucial for firms with a weak reputation (Joinson *et al.*, 2010). More specifically, a lack of justification regarding the origin of the information in personalized banner ads only makes consumers feel vulnerable on untrustworthy websites, such as Facebook (Aguirre *et al.*, 2015). Likewise, as a strong reputation already convinces consumers to accept information collection, providing a monetary compensation becomes less effective or even ineffective in convincing consumers to disclose information (Xie *et al.*, 2006).

Besides signaling benevolence and integrity, the reputation of a firm might also allude to competence and ability to provide consumers

with valuable products and services (McKnight *et al.*, 2002). Having a reputation of competence may therefore enhance the influence of the potential benefits of collection, storage, and use of information, as consumers were more convinced that personalization is valuable when it is provided by firms with a strong reputation (Bleier and Eisenbeiss, 2015b). Future research should focus on providing a better understanding how the influence of privacy practices on consumers is moderated by firm characteristics.

8

Consumer Characteristics

8.1 General privacy concern

Consumers differ in the extent to which they value their privacy (Laufer and Wolfe, 1977; Larson and Bell, 1988), implying that some consumers worry more about their privacy in general than others. This differs between generations, with older consumers being more concerned about their privacy (Bellman *et al.*, 2004; Goldfarb and Tucker, 2012). For the recent generations Y and Z digitalization and the collection of personal information has become part of everyday life, making them less reluctant towards firms collecting and using information about them. Future research should address how the change in generations will impact the distinction between "real life" and "virtual life" and how it affects the way consumers handle their privacy (see also Section 2.3).

Moreover, females (Bellman *et al.*, 2004; Goldfarb and Tucker, 2012) and consumers with less education (Milne and Boza, 1999) are generally more apprehensive about their privacy, as are consumers who have experienced a privacy violation (Bansal *et al.*, 2015; Mosteller and Poddar, 2017). Having experience with more channels or devices has both been linked to higher (Sheehan and Hoy, 2000) and lower privacy concern (Bellman *et al.*, 2004). While experienced consumers are more

aware of the risks (higher privacy concern), they also understand how to protect against these risks (lower privacy concern). Future work should explore the role of (digital) experience in more detail.

Evidently, consumers who worry more about their privacy in general are less willing to disclose information (Premazzi *et al.*, 2010; Zhao *et al.*, 2012) and more inclined to protect their privacy (Korzaan and Boswell, 2008; Milne and Culnan, 2004). Moreover, they are less receptive to products and services that rely on collecting personal information, such as loyalty programs, CRM, and behavioral targeting (Schumann *et al.*, 2014; Ashley *et al.*, 2011; Taylor *et al.*, 2015; Awad and Krishnan, 2006). Based on general privacy concern consumers have been divided into three segments: privacy fundamentalists, privacy pragmatists, and those unconcerned about privacy (Westin, 1967; Dolnicar and Jordaan, 2007; Hogan *et al.*, 2002; Ackerman *et al.*, 1999; Kumaraguru and Cranor, 2005). However, segmenting consumers based on (general) privacy concern is much disputed (Hoofnagle and Urban, 2014; Martin and Nissenbaum, 2016a), as several context- and situation-specific elements prevent these segments from accurately differentiating how consumers behave (Acquisti and Grossklags, 2005b; Urban and Hoofnagle, 2014; King, 2014). While an extensive discussion on privacy segmentation is out of the scope of this paper, future research should examine segmenting based on (general) privacy preferences more thoroughly.

As general privacy concern reflects the importance of privacy (involvement) for consumers (Bansal *et al.*, 2015; Bansal *et al.*, 2008), it could also moderate the influence of firms' privacy practices. The (positive) influence of personalized service is weaker for consumers who are highly concerned about their privacy (Shen and Dwayne Ball, 2009), while the (negative) influence of information sensitivity is stronger for these consumers (Mothersbaugh *et al.*, 2012). Moreover, highly involved consumers are more affected by transparency and other privacy-protective features (Awad and Krishnan, 2006; Bansal *et al.*, 2008), although they are not convinced by *weak* privacy signals such as privacy seals (Kim and Kim, 2011). Future research should assess in more detail whether general privacy concern enhances or diminishes the effect of privacy protective features.

8.2 Innovativeness, propensity to trust, and personal characteristics

Besides privacy concern, several other consumer-specific characteristics affect how consumers deal with firms' privacy practices. For example, innovative consumers are more inclined to accept innovations than others, also when these innovations are contingent on the collection and use of information (Xu *et al.*, 2009; Xu *et al.*, 2011; Zhao *et al.*, 2012). In fact, innovative consumers are more receptive to firms collecting and using their information in general (Mothersbaugh *et al.*, 2012; Xu *et al.*, 2011). The same holds for consumers with a high propensity to trust others (Malhotra *et al.*, 2004; Mothersbaugh *et al.*, 2012; Dinev and Hart, 2006; Hui *et al.*, 2007), as they are more convinced that firms will not misuse or exploit their information (Aljukhadar *et al.*, 2010; Kim *et al.*, 2009).

Furthermore, consumers' personal circumstances affect the influence of firms' privacy practices. Whether a consumer considers information to be sensitive may be based on his or her personal situation, with the importance of keeping information away from firms dependent on the extent to which a consumer believes he or she has something to hide. For example, while most consumers are unwilling to disclose medical information, a consumer in poor health may feel particularly strongly about this issue (Bansal *et al.*, 2010). A better understanding how a consumer's personal circumstances affect the influence of a firm's privacy practices would be highly valuable for firms.

8.3 Relationship with firm

Besides consumers' personality and personal circumstances, also their relationship with firms matters. Whether consumers trust a firm, and thus accept information collection and use, revolves around their prior experience with that firm (Schoenbachler and Gordon, 2002; Bansal *et al.*, 2015; Bart *et al.*, 2005; Chellappa and Sin, 2005).

However, even though consumers are generally more willing to disclose information to a firm they have a (long) relationship with, they are less willing to disclose embarrassing information to these

firms for fear of losing face (White, 2004). Moreover, offering monetary compensation makes consumers with positive experiences with a firm less inclined to disclose information (Premazzi *et al.*, 2010). One reason for this negative effect, which demands further investigation, could be that providing monetary compensation makes information disclosure more of a financial decision than a decision based on mutual trust. Therefore, offering monetary compensation when consumers have had positive prior experiences might give them the feeling that information disclosure is not in their best interest.

9

Environment Characteristics

9.1 Cultural differences

Privacy and privacy concern relate to cultural differences, as consumers in individualistic countries worry more about their privacy (Milberg *et al.*, 2000), making perceived privacy and security (more) important drivers for the perceived value of a website (Steenkamp and Geyskens, 2006). However, in a more recent study individualism has also been linked to a lower privacy concern (Lowry *et al.*, 2011). Therefore, more insights on the influence of culture on privacy (concern) are required.

Importantly, consumers from different countries and cultures worry about different issues (Gurau and Ranchhod, 2009; Miltgen and Peyrat-Guillard, 2014). For example, for US consumers unauthorized secondary use is a minor issue, whereas for Singaporean consumers this is the most important privacy violation when dealing with online retailers (Hann *et al.*, 2007). Since most knowledge is based on US-based samples, future work should aim to include consumers from outside the United States to assess these differences in more detail.

9.2 Legislation

National differences are also reflected in legislation (Bellman *et al.*, 2004; Milberg *et al.*, 2000). In countries for which the rule of law is very formal and strict, privacy and security features are less important drivers for the perceived value of a website (Steenkamp and Geyskens, 2006). Moreover, while US legislation is focused on letting firms and consumers negotiate fairly over the collection, storage, and use of personal information (Ohlhausen, 2014), the European Union has become more protective over the past decade, as evidenced by the upcoming General Data Protection Regulation. As these differences affect firms' potential to collect, store, and use information (Goldfarb and Tucker, 2011b), focusing on consumers' individual wishes is not enough, as firms' privacy practices should also be in line with national laws (Nissenbaum, 2004). While discussing privacy legislation and its influence on firms is out of scope, future research should carefully assess how both current and future privacy legislation affect firms' privacy practices.

Consumers are not always aware how legislation protects their privacy. Nevertheless, since consumers worry less when they believe they are protected by the law, they become more willing to provide information, less inclined to fabricate information, and less inclined to actively protect their privacy (Lwin *et al.*, 2007). Moreover, while it has been suggested that the presence of legislation becomes less important when firms provide control (Xu *et al.*, 2009), another study suggests the effect is the other way around — providing control becomes less effective in the presence of legislation (Xu *et al.*, 2012b). Future research should examine this interplay between privacy legislation and control, and its influence on consumers, in more detail.

9.3 Privacy-enhancing technologies

Consumers have recently begun taking matters in their own hands by using privacy-enhancing technologies (PETs) that offer options for privacy, such as browser extensions and ad or cookie blockers. Even when not all consumers have access to these technologies, we expect they

will affect how privacy practices influence consumers. As an example, giving consumers control would be less effective when consumers are able to use PETs that provide them control over the collection, storage, or use of information. While prior studies have assessed what determines whether PETs are used (e.g., perceived ease-of-use, perceived usefulness) (Xu *et al.*, 2012a), understanding how these PETs affect firms and the relationships with their customers remains an important area for future research.

10

Summary and Directions for Future Research

As firms increasingly collect, store, and use information about consumers, privacy concerns have surged. Given the importance of consumer information to firms, understanding how privacy affects consumers is crucial. Drawing on insights from various fields, we review relevant findings with regard to the effect of firms' privacy practices on consumers. Table 10.1 provides an overview of these findings. Table 10.2 describes how some of these effects are moderated by differences between firms, consumers, and environments.

On the basis of this review, we have formulated several hypotheses with regard to the influence of firms' privacy practices that should provide direction for future research. On a more general level, more research should be devoted to how consumers trade off the negative and positive consequences of information disclosure (the privacy calculus) in specific contexts, and in which circumstances consumers behave in accordance with this tradeoff. Future research should (1) identify the negative and positive consequences of information collection, storage, and use, (2) assess the extent to which consumers are aware of these consequences, (3) reveal the impact of these consequences, and (4) use field studies to link these consequences to relevant behavioral outcomes,

Table 10.1: Current knowledge about consumer privacy (main effects).

Topic	Findings	Main papers
Information collection	— Consumers are less inclined to disclose information when firms request more (sensitive) information — Consumers are more inclined to accept information collection by computers than humans (e.g., employers) — Consumers are more inclined to disclose information when they receive monetary compensation, although this response depends on the type of information and the amount of compensation — Consumers are more inclined to disclose information when firms disclose information first, when privacy (concern) is not triggered, or when other consumers disclose similar information	Acquisti *et al.* (2012), Acquisti *et al.* (2013), Hui *et al.* (2007), Martin *et al.* (2017), Milne *et al.* (2017), Mothersbaugh *et al.* (2012), Premazzi *et al.* (2010), Schwaig *et al.* (2013), and White (2004)
Information storage	— Consumers worry that unknown outsiders may get access to their personal information — Privacy breaches, both the firm's own and that of a competitor, can negatively affect stock prices	Acquisti *et al.* (2006), Martin *et al.* (2017), and Sutanto *et al.* (2013)
Information use	— Consumers are affected less when information is used at an aggregated level — Consumers value personalization less when it demands they have to provide additional information or when it is based on sensitive information — Consumers click (and buy) more when banner ads and direct mail are personalized, unless these ads or mails arouse privacy concerns by making it obvious that firms collect, store, and use consumers' information — Consumers are less committed and loyal to firms that share or sell information with (unknown) third parties	Bleier and Eisenbeiss (2015a), Bleier and Eisenbeiss (2015b), Goldfarb and Tucker (2011b), Coelho and Henseler (2012), Lambrecht and Tucker (2013), Tucker (2014), Wirtz and Lwin (2009), Xie *et al.* (2006), Xu *et al.* (2009), Xu *et al.* (2011), and Zhao *et al.* (2012)

(*Continued*)

Table 10.1: (*Continued*)

Topic	Findings	Main papers
Transparency	— Consumers are more committed and cooperative towards transparent firms — Consumers do not always take the time to understand how firms handle their privacy, and use privacy statements (and seals) as heuristics instead — Consumers do not always think about privacy, which is why privacy statements (or other sensitive terms) can arouse consumers' privacy concerns — Consumers are more inclined to accept information collection, storage, and use when firms explain the (right) benefits to them	Aguirre *et al.* (2015), Aiken and Boush (2006), Aljukhadar *et al.* (2010), Hui *et al.* (2007), Martin *et al.* (2017), Schumann *et al.* (2014), Son and Kim (2008), Tsai *et al.* (2011), and Wirtz and Lwin (2009)
Control	— Consumers are more inclined to choose a firm, disclose sensitive information, or accept personalized ads when (they believe) firms provide control over the collection, storage, and use of information — Consumers accept information collection more often when firms make information collection the default (e.g., opt-out choice)	Acquisti *et al.* (2013), Johnson *et al.* (2002), Martin *et al.* (2017), Mothersbaugh *et al.* (2012), Schumann *et al.* (2014), and Tucker (2014)

ranging from accepting information collection to churn and word of mouth. Except for some recent studies on online advertising, most findings are based on scenarios and intentions rather than actual behavior. Linking consumers' privacy calculus or their intentions to actual behavior should also result in a better understanding of when and why the privacy paradox occurs or whether it is due to inherently inconsistent consumer behavior.

Besides being challenged by the collection, storage, and use of personal information, increasing regulatory and technological pressure forces firms to better understand the role of transparency and control. Although one could debate whether informed consent works in practice

Table 10.2: Current knowledge about consumer privacy (moderators).

Moderator	Findings	Main papers
Firm	— The effect of privacy-protective and -invasive features on consumers is more pronounced in industries that rely on collecting sensitive information — The effect of information sensitivity is less pronounced when the information is congruent with the firm's products and services — The effect of monetary compensation on consumers is weaker (or absent) for firms with a strong reputation	Aguirre *et al.* (2015), Bart *et al.* (2005), Lwin *et al.* (2007), Pan and Zinkhan (2006), and Xie *et al.* (2006)
Consumer	— The effect of information sensitivity and privacy-protective features (e.g., transparency) is more pronounced for consumers with a high general privacy concern — The effect of the benefits of data-driven innovations is stronger for consumers high on innovativeness — The effect of monetary compensation on consumers' willingness to disclose information is weaker (or absent) when consumers already have a relationship with a firm	Bansal *et al.* (2015), Bansal *et al.* (2010), Premazzi *et al.* (2010), Mothersbaugh *et al.* (2012), White (2004), Xu *et al.* (2009), Xu *et al.* (2011), and Zhao *et al.* (2012)
Environment	— The effect of privacy-protective and privacy-invasive features on consumers depends on cultural differences — The effect of control on consumers is less pronounced in countries with strong privacy legislation or in the presence of privacy-enhancing technologies (PETs)	Hann *et al.* (2007), Lwin *et al.* (2007), Steenkamp and Geyskens (2006), Xu *et al.* (2009), Xu *et al.* (2011), and Zhao *et al.* (2012)

(Landau, 2015; Nissenbaum, 2015), it appears to remain the main focus of legislators, both in the United States and the European Union. Therefore, future research should provide insights into (1) the extent to which transparency and control affect actual consumer behavior, (2)

in which situations and for which firms and consumers transparency and control are crucial, (3) in which form firms should provide transparency and control, and (4) the long-term consequences of providing transparency and control. Game-theoretic models suggest that proactive privacy protection is a viable business model (Lee *et al.*, 2011). However, given the drawbacks of transparency and control, it remains to be seen whether this also works in practice.

Finally, future research should focus on the differences between consumers and environments. Younger generations seem less concerned about the collection of information, which might have a profound influence on the way consumers handle their privacy. Another issue is that most studies so far have used student samples from the United States to show how firms' privacy practices affect consumers. However, given the differences between generations — for example, older consumers are more concerned — these findings might not be generalizable. Likewise, given that cultural differences exist with regard to privacy — for example, loss of face is more important in Asian culture — cross-cultural studies need to assess how these differences moderate the effect of firms' privacy practices on consumers.

10.1 Managerial implications

On the basis of current knowledge summarized in Tables 2 and 3, we identify five important managerial implications for firms. First, firms must exercise caution about *what* information they collect and *how*. Consumers are not only hesitant to disclose sensitive information, such as financial or medical information, but are less responsive to monetary compensation or any other means to convince them to accept information collection. Moreover, while collecting information automatically is more convenient for consumers, these same consumers might also consider it as unfair.

Second, firms should make sure that their information storage is secure. Security breaches reduce firm value (i.e., stock prices), and by damaging a firm's reputation it might also hurt firms in the long run. In addition to preventing security breaches, firms could attempt to decrease the negative impact of any security breach, for example, by being

transparent in their communication and providing control via adequate channels. Also anonymization of stored information could decrease the risks for consumers, although this only helps when consumers understand that anonymization puts them less at risk.

Third, firms should be aware that the acceptance of profiling and personalization depends on which and how much information is used. Employing personal information in personalized banner ads or direct mailings could trigger privacy concern (and reactance), which could reduce the effectiveness of these ads or mailings. Yet, firms should also be aware of how the use of information, in particular for personalization, could provide consumers with the convenience of receiving (relevant) content at the right time and location. Overall, a thorough understanding of the benefits and costs of information use for personalization and other purposes is essential for firms.

Fourth, although firms should ensure that they handle privacy honestly, firms have to take into account that transparency — that is, communicating about privacy — triggers privacy concerns. Therefore, firms should only mention privacy when consumers have an actual privacy decision to make (e.g., whether to allow information collection), as transparency works best in concurrence with control. Moreover, rather than (only) convincing consumers they are not at risk, firms should be transparent about how the collection, storage, and use of information benefits consumers.

Finally, for all of these implications holds that firms have to take into account that the influence of privacy practices differs between firms, consumers, and environments. In particular, firms have to be aware that privacy is a more pressing issue in industries that handle either a lot of information or sensitive information. Moreover, firms should realize that some consumers value their privacy more than others, which affects whether they accept information collection, and therefore also the adoption of data-driven products and services. In understanding consumer behavior, it is important to take into account that consumers' privacy preferences are both situation- and context-specific.

10.2 Conclusion

Consumer informational privacy affects firms on the strategic and operational levels regarding product management (e.g., personalization), distribution (e.g., location-based services), pricing (e.g., monetary benefits for providing information), and communication (e.g., transparency). In recent years, collecting information about consumers has become crucial for firms. However, as the growing collection of information has triggered consumers' privacy concerns, understanding how privacy affects consumers has shifted from being a minor issue to being an area in great need of more insights. By summarizing current knowledge and formulating hypotheses about the influence of firms' privacy practices, we provide direction to future research. Although the concept of privacy has changed and will change over time, it will remain an important issue for many years to come.

References

Ackerman, M. S., L. F. Cranor, and J. Reagle (1999). "Privacy in e-commerce: Examining user scenarios and privacy preferences". *ACM Conf. Electron. Commer.* DOI: 10.1145/336992.336995.

Acquisti, A., L. Brandimarte, and G. Loewenstein (2015). "Privacy and human behavior in the age of information". *Science*. 347: 509–514.

Acquisti, A., A. Friedman, and R. Telang (2006). "In *WEIS*". Available at: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf.

Acquisti, A. and J. Grossklags (2005a). "In *WEIS*". Available at: http://www.infosecon.net/workshop/pdf/64.pdf, pp. 1–21.

Acquisti, A. and J. Grossklags (2005b). "Privacy and rationality in individual decision making". *Secur. Privacy, IEEE*. 3. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1392696.

Acquisti, A., L. K. John, and G. Loewenstein (2012). "The impact of relative standards on the propensity to disclose". *J. Mark. Res.* 49: 160–174.

Acquisti, A., L. K. John, and G. Loewenstein (2013). "What is privacy worth?" *J. Legal Stud.* 42: 249–274.

Acquisti, A., C. R. Taylor, and L. Wagman (2016). "The economics of privacy". *J. Econ. Lit.* 54: 442–492.

Acquisti, A. and H. R. Varian (2005). "Conditioning prices on purchase history". *Mark. Sci.* 24: 367–381.

Adjerid, I., A. Acquisti, R. Telang, R. Padman, and J. Adler-Milstein (2016). "The impact of privacy regulation and technology incentives: The case of health information exchanges". *Manage. Sci.* DOI: 10.1287/mnsc.2015.2194.

Adomavicius, G. and A. Tuzhilin (2005). "Personalization technologies". *Commun. ACM.* 48: 83–90.

Aguirre, E., D. Mahr, D. Grewal, K. de Ruyter, and M. Wetzels (2015). "Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness". *J. Retail.* 91: 34–49.

Aiken, K. D. and D. M. Boush (2006). "Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals". *J. Acad. Mark. Sci.* 34: 308–323.

Aljukhadar, M., S. Senecal, and D. Ouellette (2010). "Can the media richness of a privacy disclosure enhance outcome? A multifaceted view of trust in rich media environments". *Int. J. Electron. Commer.* 14: 103–126.

Alreck, P. L. and R. B. Settle (2007). "Consumer reactions to online behavioural tracking and targeting". *J. Database Mark. Cust. Strateg. Manag.* 15: 11–23.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Monterey, CA: Brooks/Cole Publishing.

Andrade, E. B., V. Kaltcheva, and B. Weitz (2002). "Self-disclosure on the web: The impact of privacy policy, reward, and company reputation". *Adv. Consum. Res.* 29: 350–354.

Ansari, A. and C. F. Mela (2003). "E-customization". *J. Mark. Res.* 40: 131–145.

Ariely, D. (2009). "The end of rational economics". *Harv. Bus. Rev.* July–Aug.

Ashley, C., S. M. Noble, N. Donthu, and K. N. Lemon (2011). "Why customers won't relate: Obstacles to relationship marketing engagement". *J. Bus. Res.* 64: 749–756.

Awad, N. F. and M. S. Krishnan (2006). "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization". *MIS Q.* 30: 13–28.

Bansal, G., F. M. Zahedi, and D. Gefen (2008). "In *ICIS 2008 Proceedings*". Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1209&context=icis2008. pp. 1–20.

Bansal, G., F. M. Zahedi, and D. Gefen (2010). "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online". *Decis. Support Syst.* 49: 138–150.

Bansal, G., F. M. Zahedi, and D. Gefen (2015). "Do context and personality matter? Trust and privacy concerns in disclosing private information online". *Inf. Manag.* 53: 1–21.

Bart, Y., V. Shankar, F. Sultan, and G. L. Urban (2005). "Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study". *J. Mark.* 69: 133–152.

Bauer, R. A. (1960). "Dynamic Marketing for a Changing World". In: ed. by R. S. Hancock. Chicago: American Marketing Association. 389–398.

Belanger, F., J. S. Hiller, and W. J. Smith (2002). "Trustworthiness in electronic commerce: The role of privacy, security, and site attributes". *J. Strateg. Inf. Syst.* 11: 245–270.

Bellman, S., E. J. Johnson, S. J. Kobrin, and G. L. Lohse (2004). "International differences in information privacy concerns: A global survey of consumers". *Inf. Soc.* 20: 313–324.

Berendt, B., O. Günther, and S. Spiekermann (2005). "Privacy in e-commerce". *Commun. ACM.* 48: 101–106.

Bleier, A. and M. Eisenbeiss (2015a). "Personalized online advertising effectiveness: The interplay of what, when, and where". *Mark. Sci.* 34: 669–688.

Bleier, A. and M. Eisenbeiss (2015b). "The importance of trust for personalized online advertising". *J. Retail.* 91: 390–409.

Bloomberg (2016). "2016 was a record year for data breaches". Available at: https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked (accessed 28 August 2017).

Bolderdijk, J. W., L. Steg, and T. Postmes (2013). "Fostering support for work floor energy conservation policies: Accounting for privacy concerns". *J. Organ. Behav.* 34: 195–210.

Boulding, W. and A. Kirmani (1993). "A consumer-side experimental examination of signaling theory: Do consumers perceive warranties as signals of quality?" *J. Consum. Res.* 20: 111–123.

Brandimarte, L., A. Acquisti, and G. Loewenstein (2013). "Misplaced confidences: Privacy and the control paradox". *Soc. Psychol. Personal. Sci.* 4: 340–347.

Brehm, J. W. (1966). *A Theory of Psychological Reactance*. Oxford, England: Academic Press.

BTG (2012). "KPN introduceert Nederlandse clouddienst". Available at: http://www.btg.org/2012/09/23/kpn-introduceert-nederlandse-clouddienst/ (accessed 28 August 2017).

Burgoon, J. K., R. Parrott, B. A. Le Poire, D. L. Kelley, J. B. Walther, and D. Perry (1989). "Maintaining and restoring privacy through communication in different types of relationships". *J. Soc. Pers. Relat.* 6: 131–158.

Caudill, E. M. and P. E. Murphy (2000). "Consumer online privacy: Legal and ethical issues". *J. Public Policy Mark.* 19: 7–19.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004). "The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers". *Int. J. Electron. Commer.* 9: 69–104.

Chaiken, S. (1980). "Heuristic Versus systematic information processing and the use of source versus message cues in persuasion". *J. Pers. Soc. Psychol.* 39: 752–766.

Chellappa, R. K. and R. G. Sin (2005). "Personalization versus privacy: An empirical examination of the online consumer's dilemma". *Inf. Technol. Manag.* 6: 181–202.

Chung, T. S., R. T. Rust, and M. Wedel (2009). "My mobile music: An adaptive personalization system for digital audio players". *Mark. Sci.* 28: 52–68.

Chung, T. S., M. Wedel, and R. T. Rust (2016). "Adaptive personalization using social networks". *J. Acad. Mark. Sci.* 44: 66–87.

CIGI-Ipsos (2017). "Global survey on internet security and trust". Available at: https://www.cigionline.org/internet-survey.

CNN (2005). "Web sites change prices based on customers' habits". Available at: http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.prices/ (accessed 28 August 2017).

Coelho, P. S. and J. Henseler (2012). "Creating customer loyalty through service customization". *Eur. J. Mark.* 46: 331–356.

Conchar, M. P., G. M. Zinkhan, C. Peters, and S. Olavarrieta (2004). "An integrated framework for the conceptualization of consumers' perceived-risk processing". *J. Acad. Mark. Sci.* 32: 418–436.

CTA (2017). "44 Percent of U.S. Online Adults Plan to Purchase a Smart Speaker". Available at: https://www.cta.tech/News/Blog/Articles/2017/December/44-Percent-of-U-S-Online-Adults-Plan-to-Purchase.aspx.

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use". *MIS Q.* 17: 341–363.

Culnan, M. J. (1995). "Consumer awareness of name removal procedures: Implications for direct marketing". *J. Direct Mark.* 9: 10–19.

Culnan, M. J. and P. K. Armstrong (1999). "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation". *Organ. Sci.* 10: 104–115.

Culnan, M. J. and R. J. Bies (2003). "Consumer privacy: Balancing economic and justice considerations". *J. Soc. Issues.* 59: 323–342.

Davis, F. D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology". *MIS Q.* 13: 319–340.

Demoulin, N. T. M. and P. Zidda (2009). "Drivers of customers' adoption and adoption timing of a new loyalty card in the grocery retail market". *J. Retail.* 85: 391–405.

Derikx, S., M. de Reuver, and M. Kroesen (2016). "Can privacy concerns for insurance of connected cars be compensated?" *Electron. Mark.* 26: 73–81.

Dinev, T. and P. Hart (2006). "An extended privacy calculus model for e-commerce transactions". *Inf. Syst. Res.* 17: 61–80.

Dinev, T., A. R. McConnell, and J. H. Smith (2015). "Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box". *Inf. Syst. Res.* 26: 639–655.

Dinev, T., H. Xu, J. H. Smith, and P. Hart (2013). "Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts". *Eur. J. Inf. Syst.* 22: 295–316.

Dolnicar, S. and Y. Jordaan (2007). "A market-oriented approach to responsibility managing information privacy concerns in direct marketing". *J. Advert.* 36: 123–149.

Donaldson, T. and T. W. Dunfee (1994). "Towards a unified conception of business ethics: Integrative social contracts theory". *Acad. Manag. Rev.* 19: 252–284.

Dorotic, M., T. H. A. Bijmolt, and P. C. Verhoef (2012). "Loyalty programmes: Current knowledge and research directions". *Int. J. Manag. Rev.* 14: 217–237.

Eastlick, M. A., S. L. Lotz, and P. Warrington (2006). "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment". *J. Bus. Res.* 59: 877–886.

Edwards, S. M., H. Li, and J.-H. Lee (2002). "Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads". *J. Advert.* 31: 83–95.

Eurobarometer (2011). "Attitudes on data protection and electronic identity in the European Union".

Featherman, M. S., A. D. Miyazaki, and D. E. Sprott (2010). "Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility". *J. Serv. Mark.* 24: 219–229.

Feinberg, F. M., A. Krishna, and Z. J. Zhang (2002). "Do we care what others get? A behaviorist approach to targeted promotions". *J. Mark. Res.* 39: 277–291.

Fishbein, M. and I. Ajzen (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addition-Wesley.

Forbes (2015). "Samsung's smart TVs share living room conversations with third parties". Available at: http://www.forbes.com/sites/parmyolson/2015/02/09/samsungs-smart-tv-data-sharing-nuance/ (accessed 28 August 2017).

Foxman, E. R. and P. Kilcoyne (1993). "Information technology, marketing practice, and consumer privacy: Ethical issues". *J. Public Policy Mark.* 12: 106–119.

Gabisch, J. A. and G. R. Milne (2014). "The impact of compensation on information ownership and privacy control". *J. Consum. Mark.* 31: 13–26.

General Data Protection Regulation (EU) (2016). "General Data Protection Regulation". European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

Goldfarb, A. and C. E. Tucker (2011a). "Online display advertising: Targeting and obtrusiveness". *Mark. Sci.* 30: 389–404.

Goldfarb, A. and C. E. Tucker (2011b). "Privacy regulation and online advertising". *Manage. Sci.* 57: 57–71.

Goldfarb, A. and C. E. Tucker (2012). "Shifts in privacy concerns". *Am. Econ. Rev.* 102: 349–353.

Goodwin, C. (1991). "Privacy: Recognition of a consumer right". *J. Public Policy Mark.* 10: 149–166.

Gurau, C. and A. Ranchhod (2009). "Consumer privacy issues in mobile commerce: A comparative study of British, French and Romanian consumers". *J. Consum. Mark.* 26: 496–507.

Hann, I.-H., K. Hui, T. S. Lee, and I. P. L. Png (2007). "Overcoming online information privacy concerns: An information-processing theory approach". *J. Manag. Inf. Syst.* 24: 13–42.

Hauser, J. R., G. Liberali, and G. L. Urban (2014). "Website morphing 2.0: Switching costs, partial exposure, random exit, and when to morph". *Manage. Sci.* 60: 1594–1616.

Heimbach, I., J. Gottschlich, and O. Hinz (2015). "The value of user's Facebook profile data for product recommendation generation". *Electron. Mark.* 25: 125–138.

Higgins, E. T. (1997). "Beyond pleasure and pain". *Am. Psychol.* 52: 1280–1300.

Hoffman, D. L., T. P. Novak, and M. Peralta (1999). "Building consumer trust online". *Commun. ACM.* 42. Available at: http://dl.acm.org/citation.cfm?id=299175.

Hogan, J. E., K. N. Lemon, and R. T. Rust (2002). "Customer equity management: Charting new directions for the future of marketing". *J. Serv. Res.* 5: 4–12.

Holtrop, N., J. E. Wieringa, M. J. Gijsenberg, and P. C. Verhoef (2017). "No future without the past? Predicting churn in the face of customer privacy". *Int. J. Res. Mark.* 34: 154–172.

Homans, G. C. (1958). "Social behavior as exchange". *Am. J. Sociol.* 63: 597–606.

Hoofnagle, C. J. and J. M. Urban (2014). "Alan Westin's Privacy Homo Economicus". Vol. 261. Available at: http://papers.ssrn.com/abstract=2434800.

Huffington Post (2017). "Smart speakers and voice recognition: Is your privacy at risk?" Available at: http://www.huffingtonpost.com/entry/smart-speakers-and-voice-recognition-is-your-privacy_us_58f14ddee4b04cae050dc73e (accessed 28 Augest 2017).

Hui, K.-L., H.-H. Teo, and T. S. Lee (2007). "The value of privacy assurance: An exploratory field experiment". *MIS Q.* 31: 19–33.

Jai, T.-M. (C.), L. D. Burns, and N. J. King (2013). "The effect of behavioral tracking practices on consumers' shopping evaluations and repurchase intention toward trusted online retailers". *Comput. Human Behav.* 29: 901–909.

John, L. K., A. Acquisti, and G. Loewenstein (2011). "Strangers on a plane: Context-dependent willingness to divulge sensitive information". *J. Consum. Res.* 37: 858–873.

Johnson, E. J., S. Bellman, and G. L. Lohse (2002). "Defaults, framing and privacy: Why opting in-opting out". *Mark. Lett.* 13: 5–15.

Joinson, A. N., U.-D. Reips, T. Buchanan, and C. B. P. Schofield (2010). "Privacy, trust, and self-disclosure online". *Human–Computer Interact.* 25: 1–24.

Khan, R., M. Lewis, and V. Singh (2009). "Dynamic customer management and the value of one-to-one marketing". *Mark. Sci.* 28: 1063–1079.

Kim, D. J., D. L. Ferrin, and H. R. Rao (2009). "Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration". *Inf. Syst. Res.* 20: 237–257.

Kim, K. and J. Kim (2011). "Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust". *J. Interact. Mark.* 25: 145–158.

King, J. (2014). "In *Symposium on Usable Privacy and Security (SOUPS)*". pp. 1–8.

Knijnenburg, B. P. and A. Kobsa (2013). "Making decisions about privacy: Information disclosure in context-aware recommender systems". In: *ACM Transactions on Interactive Intelligent Systems*. Available at: https://www.ics.uci.edu/~kobsa/papers/2013-TIIS-Kobsa.pdf. 1–33.

Knijnenburg, B. P., A. Kobsa, and H. Jin (2013). "Dimensionality of information disclosure behavior". *Int. J. Hum. Comput. Stud.* 71: 1144–1162.

Korzaan, M. L. and K. T. Boswell (2008). "The influence of personality traits and information privacy concerns on behavioral intentions". *J. Comput. Inf. Syst.* 48: 15–24.

Kumaraguru, P. and L. F. Cranor (2005). "Privacy indexes: A survey of Westin's studies". Available at: http://repository.cmu.edu/isr/856/.

Lacey, R., J. Suh, and R. M. Morgan (2007). "Differential effects of preferential treatment levels on relational outcomes". *J. Serv. Res.* 9: 241–256.

Lambrecht, A. and C. E. Tucker (2013). "When does retargeting work? Information specificity in online advertising". *J. Mark. Res.* 50: 561–576.

Landau, S. (2015). "Control use of data to protect privacy". *Science.* 347: 504–506.

Lanier, C. D. and A. Saini (2008). "Understanding consumer privacy: A review and future directions". *Acad. Mark. Sci. Rev.* 12. Available at: http://www.kommunikationsforum.dk/Profiler/ProfileFolders/Kkort/Understanding.pdf.

LaRose, R. and N. J. Rifon (2007). "Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior". *J. Consum. Aff.* 41: 127–150.

Larson, J. H. and N. J. Bell (1988). "Need for privacy and it's effect upon interpersonal attraction and interaction". *J. Soc. Clin. Psychol.* 6: 1–10.

Laufer, R. S. and M. Wolfe (1977). "Privacy as a concept and a social issue: A multidimensional developmental theory". *J. Soc. Issues.* 33. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1540-4560.1977.tb01880.x/abstract.

Lee, D.-J., J.-H. Ahn, and Y. Bang (2011). "Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection". *MIS Q.* 35: 423–444.

Leenheer, J., H. J. Van Heerde, T. H. A. Bijmolt, and A. Smidts (2007). "Do loyalty programs really enhance behavioral loyalty? An empirical analysis accounting for self-selecting members". *Int. J. Res. Mark.* 24: 31–47.

Li, H., S. M. Edwards, and J.-H. Lee (2002). "Measuring the intrusiveness of advertisements: Scale development and validation". *J. Advert.* 31: 37–47.

Li, H., R. Sarathy, and H. Xu (2010). "Understanding situational online information disclosure as a privacy calculus". *J. Comput. Inf. Syst.* 51: 1–29.

Lowry, P. B., J. Cao, and A. Everard (2011). "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures". *J. Manag. Inf. Syst.* 27: 163–200.

Luo, X., M. Andrews, Z. Fang, and C. W. Phang (2014). "Mobile targeting". *Mark. Sci.* 60: 1738–1756.

Lwin, M. O., J. Wirtz, and A. J. S. Stanaland (2016). "The privacy dyad". *Internet Res.* 26: 919–941.

Lwin, M. O., J. Wirtz, and J. D. Williams (2007). "Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective". *J. Acad. Mark. Sci.* 35: 572–585.

Malhotra, A. and C. Kubowicz Malhotra (2011). "Evaluating customer information breaches as service failures: An event study approach". *J. Serv. Res.* 14: 44–59.

Malhotra, N. K., S. S. Kim, and J. Agarwal (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model". *Inf. Syst. Res.* 15: 336–355.

Martin, K. D., A. Borah, and R. W. Palmatier (2017). "Data privacy: Effects on customer and firm performance". *J. Mark.* 81: 36–58.

Martin, K. D. and P. E. Murphy (2017). "The role of data privacy in marketing". *J. Acad. Mark. Sci.* 45: 135–155.

Martin, K. E. and H. Nissenbaum (2016a). "Measuring privacy: An empirical test using context to expose confounding variables". *Columbia Sci. Technol. Law Rev.* 18: 176–2018.

Martin, K. E. and H. Nissenbaum (2016b). "Measuring privacy: Using context to expose confounding variables". *Columbia Sci. Technol. Law Rev.* 18: 1–40.

Mason, R. O. (1986). "Four ethical issues of the information age". *MIS Q.* 10: 5–12.

McKnight, D. H., V. Choudhury, and C. Kacmar (2002). "Developing and validating trust measures for e-commerce: An integrative typology". *Inf. Syst. Res.* 13: 334–359.

Metzger, M. J. (2007). "Communication privacy management in electronic commerce". *J. Comput. Mediat. Commun.* 12: 1–27.

Milberg, S. J., J. H. Smith, and S. J. Burke (2000). "Information privacy: Corporate management and national regulation". *Organ. Sci.* 11: 35–57.

Miller, A. R. and C. E. Tucker (2009). "Privacy protection and technology diffusion: The case of electronic medical records". *Manage. Sci.* 55: 1077–1093.

Milne, G. R. and M.-E. Boza (1999). "Trust and concern in consumers' perceptions of marketing information management practices". *J. Interact. Mark.* 13: 5–24.

Milne, G. R. and M. J. Culnan (2004). "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices". *J. Interact. Mark.* 18: 15–29.

Milne, G. R. and M. E. Gordon (1993). "Direct mail privacy-efficiency trade-offs within an implied social contract framework". *J. Public Policy Mark.* 12: 206–215.

Milne, G. R., G. Pettinico, F. M. Hajjat, and E. Markos (2017). "Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing". *J. Consum. Aff.* 51: 133–161.

Miltgen, C. L. and D. Peyrat-Guillard (2014). "Cultural and generational influences on privacy concerns: A qualitative study in seven European countries". *Eur. J. Inf. Syst.* 23: 103–125.

Montgomery, A. L. and M. D. Smith (2009). "Prospects for personalization on the Internet". *J. Interact. Mark.* 23: 130–137.

Moon, Y. (2000). "Intimate exchanges: Using computers to elicit self-disclosure from consumers". *J. Consum. Res.* 26: 323–339.

Morgan, R. M. and S. D. Hunt (1994). "The commitment-trust theory of relationship marketing". *J. Mark.* 58: 20–38.

Mosteller, J. and A. Poddar (2017). "To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors". *J. Interact. Mark.* 39: 27–38.

Mothersbaugh, D. L., W. K. Foxx, S. E. Beatty, and S. Wang (2012). "Disclosure antecedents in an online service context: The role of sensitivity of information". *J. Serv. Res.* 15: 76–98.

Nissenbaum, H. (2004). "Privacy as contextual integrity". *Washingt. Law Rev.* 79: 101–139.

Nissenbaum, H. (2015). "Respecting context to protect privacy: Why meaning matters". *Sci. Eng. Ethics.* DOI: 10.1007/s11948-015-9674-9.

Norberg, P. A. and D. R. Horne (2014). "Coping with information requests in marketing exchanges: An examination of pre-post affective control and behavioral coping". *J. Acad. Mark. Sci.* 42: 415–429.

Norberg, P. A., D. R. Horne, and D. A. Horne (2007). "The privacy paradox: Personal information disclosure intentions versus behaviors". *J. Consum. Aff.* 41: 100–127.

Nowak, G. J. and J. E. Phelps (1995). "Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters". *J. Direct Mark.* 9: 46–60.

Ohlhausen, M. K. (2014). "Privacy challenge and opportunities: The role of the Federal Trade Commission". *J. Public Policy Mark.* 33: 4–9.

Olmstead, K. and M. Atkinson (2015). "Apps permissions in the Google Play Store".

Pan, Y. and G. M. Zinkhan (2006). "Exploring the impact of online privacy disclosures on consumer trust". *J. Retail.* 82: 331–338.

Parasuraman, A., V. A. Zeithaml, and A. Malhotra (2005). "E-S-QUAL: A multiple-item scale for assessing electronic service quality". *J. Serv. Res.* 7: 213–233.

Pavlou, P. A. (2011). "State of the information privacy literature: where are we and where should we go?" *MIS Q.* 35: 977–988.

Peltier, J. W., G. R. Milne, and J. E. Phelps (2009). "Information privacy research: Framework for integrating multiple publics, information channels, and responses". *J. Interact. Mark.* 23: 191–205.

Peter, J. P. and L. X. Tarpey (1975). "A comparative analysis of three consumer decision strategies". *J. Consum. Res.* 2: 29–37.

Petronio, S. (1991). "Communication boundary management: A theoretical model of managing disclosure of private information between marital couples". *Commun. Theory.* 1: 311–335.

Petty, R. E. and J. T. Cacioppo (1986). "The elaboration likelihood model of persuasion". *Adv. Exp. Soc. Psychol.* 19: 123–205.

Phelps, J. E., G. J. Nowak, and E. Ferrell (2000). "Privacy concerns and consumer willingness to provide personal information". *J. Public Policy Mark.* 19: 27–41.

Posner, R. A. (1978). "An economic theory of privacy". *Georg. Law Rev.* 19–26.

Posner, R. A. (1981). "The economics of privacy". *Am. Econ. Rev.* 71: 405–409.

Premazzi *et al.*, K. (2010). "Customer information sharing with e-vendors: The roles of incentives and trust". *Int. J. Electron. Commer.* 14: 63–91.

Prosser, W. L. (1960). "Privacy". *Calif. Law Rev.* 48: 383–423.

Purcell, K., J. Brenner, and L. Rainie (2012). "Search engine use". DOI: 10.1016/j.chb.2011.10.002.

Reinsel, D., J. Gantz, and J. Rydning (2017). "Data age 2025". Available at: http://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

Rifon, N. J., R. LaRose, and S. M. Choi (2005). "Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures". *J. Consum. Aff.* 39: 339–362.

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change". *J. Psychol.* 91: 9–114.

Rust, R. T. and M.-H. Huang (2014). "The service revolution and the transformation of marketing science". *Mark. Sci.* 33: 206–221.

Rust, R. T., P. K. Kannan, and N. Peng (2002). "The customer economics of internet privacy". *J. Acad. Mark. Sci.* 30: 455–464.

Schlosser, A. E., T. B. White, and S. M. Lloyd (2006). "Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions". *J. Mark.* 70: 133–148.

Schneider, M. J., S. Jagpal, S. Gupta, S. Li, and Y. Yu (2017). "Protecting customer privacy when marketing with second-party data". *Int. J. Res. Mark.* 1–11.

Schoenbachler, D. D. and G. L. Gordon (2002). "Trust and customer willingness to provide information in database-driven relationship marketing". *J. Interact. Mark.* 16: 2–16.

Schumann, J. H., F. Von Wangenheim, and N. Groene (2014). "Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services". *J. Mark.* 78: 59–75.

Schwaig, K. S., A. H. Segars, V. Grover, and K. D. Fiedler (2013). "A model of consumers' perceptions of the invasion of information privacy". *Inf. Manag.* 50: 1–12.

Sheehan, K. B. and M. G. Hoy (2000). "Dimensions of privacy concern among online consumers". *J. Public Policy Mark.* 19: 62–73.

Shen, A. and A. Dwayne Ball (2009). "Is personalization of services always a good thing? Exploring the role of technology-mediated personalization (TMP) in service relationships". *J. Serv. Mark.* 23: 79–91.

Slovic, P. (2000). "What does it mean to know a cumulative risk? Adolescents' perceptions of short-term and long-term consequences of smoking". *J. Behav. Decis. Mak.* 13: 249–266.

Smith, J. H., T. Dinev, and H. Xu (2011). "Information privacy research: An interdisciplinairy review". *MIS Q.* 35: 989–1015.

Smith, J. H., S. J. Milberg, and S. J. Burke (1996). "Information privacy: Measuring individuals' concerns about organizational practices". *MIS Q.* 20: 167–196.

Smith, J. S., M. R. Gleim, S. G. Robinson, W. J. Kettinger, and S.-H. Park (2014). "Using an old dog for new tricks: A regulatory focus perspective on consumer acceptance of RFID applications". *J. Serv. Res.* 17: 85–101.

Solove, D. J. (2006). "A taxonomy of privacy". *Univ. PA. Law Rev.* 154: 477–564.

Son, J.-Y. and S. S. Kim (2008). "Internet users' information privacy-protective responses: A taxonomy and a nomological model". *MIS Q.* 32: 503–529.

Spärck Jones, K. (2003). "Privacy: What's different now?" *Interdiscip. Sci. Rev.* 28. Available at: http://www.maneyonline.com/doi/abs/10.1179/030801803225008677.

Steenkamp, J.-B. E. M. and I. Geyskens (2006). "How country characteristics affect the perceived value of web sites". *J. Mark.* 70: 136–150.

Stone, E. F., H. G. Gueutal, D. G. Gardner, and S. McClure (1983). "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations". *J. Appl. Psychol.* 68: 459–468.

Sutanto, J., E. Palme, C.-H. Tan, and C. W. Phang (2013). "Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users". *MIS Q.* 37: 1141–1164.

Taylor, J. F., J. Ferguson, and P. S. Ellen (2015). "A multi-level model of individual information privacy beliefs". *J. Consum. Mark.* 32: 99–112.

Tourangeau, R. and T. Yan (2007). "Sensitive questions in surveys". *Psychol. Bull.* 133: 859–883.

TRUSTe (2016). "U.S. consumer privacy index". Available at: https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/.

Tsai, J. Y., S. Egelman, L. F. Cranor, and A. Acquisti (2011). "The effect of online privacy information on purchasing behavior: An experimental study". *Inf. Syst. Res.* 22: 254–268.

Tucker, C. E. (2014). "Social networks, personalized advertising, and privacy controls". *J. Mark. Res.* 51: 546–562.

Turow, J., J. King, C. J. Hoofnagle, A. Bleakley, and M. Hennessy (2009). "Americans reject tailored advertising and three activities that enable it".

Urban, J. M. and C. J. Hoofnagle (2014). "In *Symposium on Usable Privacy and Security (SOUPS)*".

Van Doorn, J. and J. C. Hoekstra (2013). "Customization of online advertising: The role of intrusiveness". *Mark. Lett.* 24: 339–351.

Verhoef, P. C., E. Kooge, and N. Walk (2016). *Creating Value with Big Data Analytics: Making Smarter Marketing Decisions*. Routledge.

Vroom, V. H. (1964). *Work and Motivation*. New York, New York, USA: Wiley.

Wang, S., S. E. Beatty, and W. Foxx (2004). "Signaling the trustworthiness of small online retailers". *J. Interact. Mark.* 18: 53–69.

Wedel, M. and P. K. Kannan (2016). "Marketing analytics for data-rich environments". *J. Mark.* 80: 97–121.

Westin, A. F. (1967). *Privacy and Freedom*. New York, NY, USA: Atheneum.

White, T. B. (2004). "Consumer disclosure and disclosure avoidance: A motivational framework". *J. Consum. Psychol.* 14: 41–51.

White, T. B., T. P. Novak, and D. L. Hoffman (2014). "No strings attached: When giving it away versus making them pay reduces consumer information disclosure". *J. Interact. Mark.* 28: 184–195.

White, T. B., D. L. Zahay, H. Thorbjørnsen, and S. Shavitt (2008). "Getting too personal: Reactance to highly personalized email solicitations". *Mark. Lett.* 19: 39–50.

Wirtz, J. and M. O. Lwin (2009). "Regulatory focus theory, trust, and privacy concern". *J. Serv. Res.* 12: 190–207.

Wolfinbarger, M. and M. C. Gilly (2003). "eTailQ: Dimensionalizing, measuring and predicting etail quality". *J. Retail.* 79: 183–198.

Xie, E., H.-H. Teo, and W. Wan (2006). "Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior". *Mark. Lett.* 17: 61–74.

Xie, J., B. P. Knijnenburg, and H. Jin (2014). "In *IUI*". Available at: http://dl.acm.org/citation.cfm?doid=2557500.2557504, pp. 189–198.

Xu, H., R. E. Crossler, and F. Bélanger (2012a). "A value sensitive design Investigation of privacy enhancing tools in web browsers". *Decis. Support Syst.* 54: 424–433.

Xu, H., X. (Robert) Luo, J. M. Carroll, and M. B. Rosson (2011). "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing". *Decis. Support Syst.* 51: 42–52.

Xu, H., H.-H. Teo, B. C. Y. Tan, and R. Agarwal (2009). "The role of push-pull technology in privacy calculus: The case of location-based services". *J. Manag. Inf. Syst.* 26: 135–173.

Xu, H., H.-H. Teo, B. C. Y. Tan, and R. Agarwal (2012b). "Research note — effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services". *Inf. Syst. Res.* 23: 1342–1363.

Youn, S. (2009). "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents". *J. Consum. Aff.* 43: 389–419.

Zhang, J. and M. Wedel (2009). "The effectiveness of customized promotions in online and offline stores". *J. Mark. Res.* 46: 190–206.

Zhao, L., Y. Lu, and S. Gupta (2012). "Disclosure intention of location-related information in location-based social network services". *Int. J. Electron. Commer.* 16: 53–89.

Zimmer, J. C., R. Arsal, M. Al-Marzouq, D. Moore, and V. Grover (2010). "Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure". *Decis. Support Syst.* 48: 395–406.